Title	Asset Valuation Method for Dependent Entities
Author(s)	Breier, Jakub
Citation	Breier, J. (2014). Asset Valuation Method for Dependent Entities. Journal of Internet Services and Information Security, 4(3), 72-81.
Date	2014
URL	http://hdl.handle.net/10220/42540
Rights	© 2014 The Author(s). This is the author created version of a work that has been peer reviewed and accepted for publication in Journal of Internet Services and Information Security, published by Innovative Information Science & Technology Research Group (ISYOU) AND Institute of Engineering - Polytechnic of Porto (ISEP/IPP) on behalf of The Author(s). It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [http://isyou.info/jisis/vol4/no3/5.htm].

Asset Valuation Method for Dependent Entities*

Jakub Breier
Physical Analysis and Cryptographic Engineering,
Temasek Laboratories@NTU
School of Physical and Mathematical Sciences, Division of Mathematical Sciences, Nanyang Technological University, Singapore
jbreier@ntu.edu.sg

Abstract

Asset analysis and valuation are important parts of the information security risk management. Outputs they produce are used in the process of risk analysis that plays a key role in securing organization's business processes. A correct analysis and valuation of assets should reveal not only their importance for the organization, but also their relationships and dependencies between each other. There is a lack of works considering asset dependencies for the risk management purposes, this part is usually left for a subjective perception of a risk analyst, who should adjust the risk values in the end.

In our work we propose a systematic approach for including asset dependencies in the asset valuation process. We inspect the relations between assets from the common security attributes point of view - confidentiality, integrity and availability. Our method should help to formalize the problem with dependent entities in the organization's model.

Keywords: information security risk management, risk analysis, asset valuation, asset dependencies

1 Introduction

Almost every organization has to use information processing facilities that significantly help in a fulfillment of organization processes. The whole information processing infrastructure is in a constant risk resulting from an exposure to various threats. The role of risk analysts and security mangers is to identify these threats and decide on implementations of countermeasures in order to minimize risks. The processes intended to implement these actions are known as the information security risk management.

Information security risk management [3] is a fundamental process conducted for the purpose of securing information assets in an organization. It provides the business with understanding of risks, allowing the decision makers to control and minimize these risks [6]. The main components of this process are stated in the ISO/IEC 27001:2013 [8], the most important are following:

- identification and valuation of assets,
- identification of legal and business requirements for the assets,
- identification of vulnerabilities and threats,
- calculation of risks,
- evaluation of the risks and implementation of countermeasures.

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 3, pp. 72-81

*This paper is an extended version of the paper "Assets Dependencies Model in Information Security Risk Management" that was presented at AsiaARES 2014 [4]

There are few standards that deliberate this process and provide recommendations for security specialists in organizations. The most popular are following:

- NIST Special Publication 800-39 [1] - it is intended to serve risk management professionals. As stated in the document, it is aimed to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. It provides general information on dealing with the risk management, technical details are stated in NIST Special Publication 800-30 [13] that contains more detailed data on risk analysis and management.

- ISO/IEC 27005:2011 standard [7] - it provides higher-level overview of risk management processes. First, it describes the purpose and implementation of these processes. In annexes are then provided evaluation tables and various entities in the model, such as threats, assets or consequences.

Asset valuation is an important part of the whole process, its outcome should determine, which assets are necessary for the organization in the meaning of contribution to business processes and price. This information is useful for the next phases, so that the security manager can focus only on important assets. There exist few papers and software tools implementing aforementioned standards. Usually, they propose simple valuation methods, based on a discrete measurement scale and qualitative approaches. For example they propose valuation in a terms of 'none', 'low', 'medium', or 'high' importance of an asset for the organization.

Asset dependencies are usually not discussed in works about asset analysis, only few of them deliberate this problem. But it can strongly affect the risk probabilities if two or more assets are dependent on each other. For example if we have a web server that was identified to have a low risk exposure, but this server is installed on a physical server that is in the building with the high risk value because of probability of natural disasters, it should be considered in a risk analysis.

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.

This paper extends our previous paper dealing with the asset dependencies [4]. In comparison to that paper we provide deeper overview of a related work, more detailed description of our model and we differentiate between physical and logical connections in the model. Also, we provide a discussion of our results.

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. Section 4 provides discussion of our method, and finally section 5 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 [17] 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 [15] 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. Bhattacharjee et al. [2] propose a quantitative methodology for enterprise information security risk analysis. They express the asset value as a function of security, business and legal and contractual requirements associated with an asset.

Leitner [9] 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.

Liu, Zhang and Wu [10] introduce another methodology for asset analysis, aimed to assess the IEC 61850-based power control systems. Their methodology is complex, it uses three levels of asset valuation - valuation of information exchange, asset valuation of function level and asset valuation of system level. However they use non-trivial mathematical methods without further discussion and the methodology is bound to power control systems so it could not be reused in other fields.

Loloei, Shahriari and Sadeghi [11] 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 [14] 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 [12] 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 buildings as a top-level nodes. 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. For better visualisation, physical entities and people are in two tones of dark grey, software applications are in light grey tone and data is white. Physical connections are drawn by solid lines and logical connections are drawn by dashed lines.

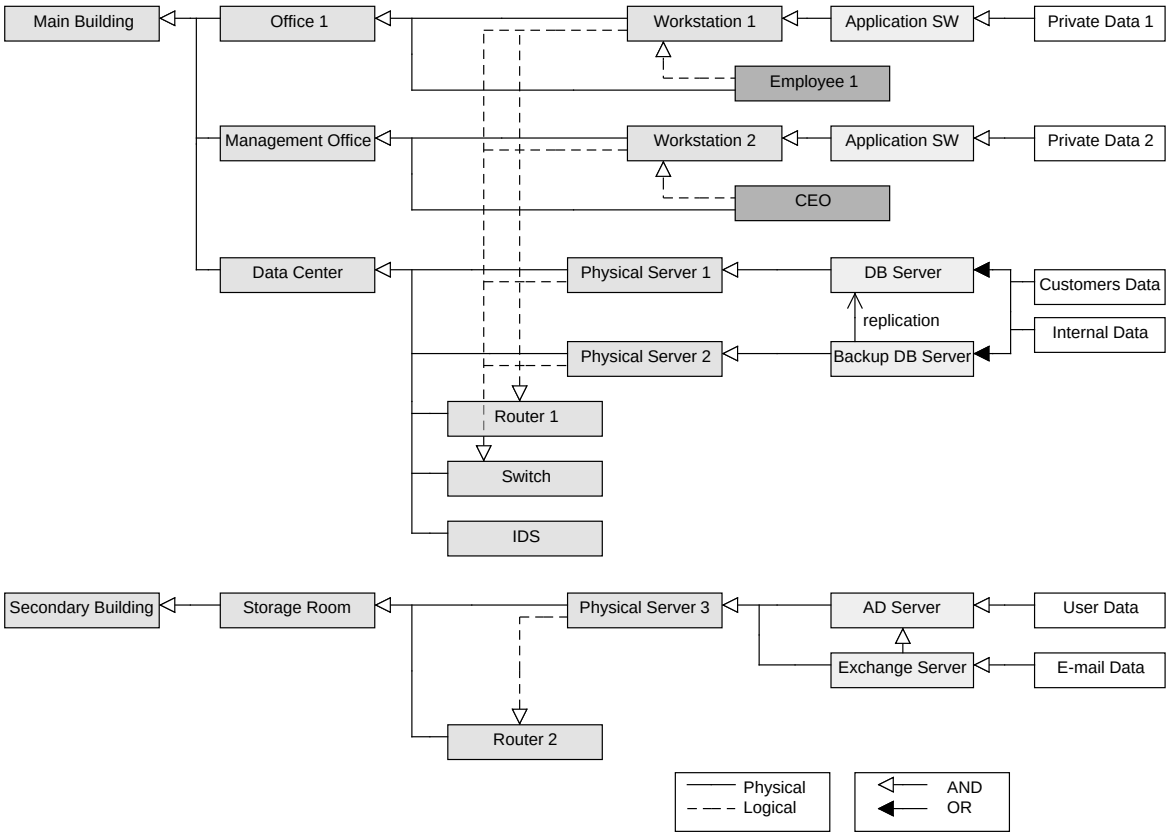

Figure 1: Dependencies between assets.

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 fol-

Table 1: Risk matrix [18].

		Probability			
		1	2	3	4
Impact	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

lowing 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 from the physical point of view and one entity from the logical point of view, 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.

- We will differentiate between physical and logical connections. Physical connection means that if an asset in upper layer in hierarchy is lost or destroyed, a dependent asset can be affected in a same way. For example, if we lose a server with data, there is a probability that this data will be lost. When considering a logical connection, dependent assets usually require assets in upper layer to work properly. For example, if some network device is malfunctioned, it will usually be a problem to communicate with servers. Logical connections have usually higher value of availability component weight.

- 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 [18] for demonstrational purposes. This matrix has threat probability for its columns and impact for its rows. Risk values are stated in Table 1. 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.

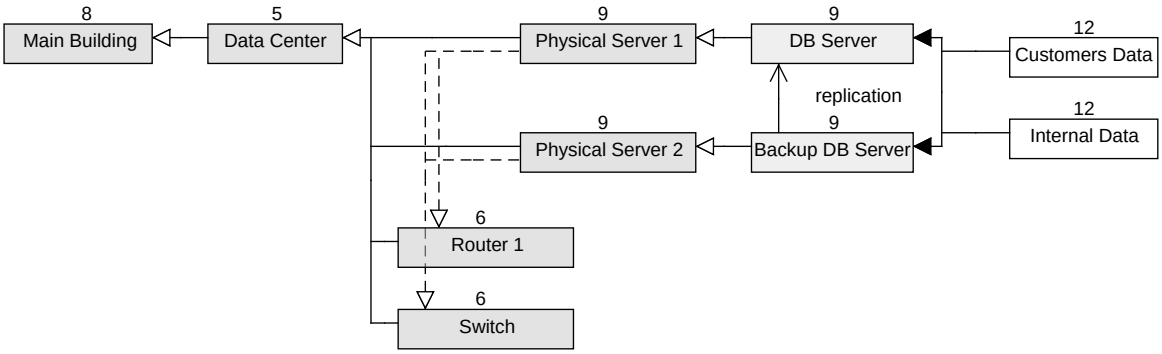

Figure 2: Risk values.

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. We differentiate between two variants of this formula, depending on the connection type (physical/logical):

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

$$AdjustmentValue(logical) = W_o \times avg(W_{con}, W_{int}, W_{ava}) \times RV \tag{3}$$

The formula depends on three factors. First, we compute the sum of the component weight values and multiply it with the maximal value among components in the case of physical dependency or with the average value in the case of logical dependency. If we consider logical connections, damaging or destroying of the upper level entity does not have physical impact on the dependent entity, that is why average value is taken into the consideration. Physical connections are stronger considering this fact, so

Table 2: Dependency adjustment formula examples.

Dependent Entity	W_o	$max(W_{con}, W_{int}, W_{ava})$	RV	Adjustment Value
Asset 1	0.7	0.3	1	**+0.21**
Asset 2	1.5	0.7	2	**+1.05**
Asset 3	1.5	1.0	2	**+3.00**
Asset 4	2.4	0.8	3	**+5.76**

Table 3: Adjusted risk values.

Dependent Entity	W_o	W_{max}	Original Risk Val.	RV	Adjusted Risk Val.
Data Center	0.8	0.5	5	2	**5.8**
Router 1	0.9	0.5	6	1	**6.45**
Switch	0.9	0.5	6	1	**6.45**
Physical Server 1 & 2 - Data Center	0.8	0.5	9	1	**9.4**
Physical Server 1 & 2 - Router 1	0.3	0.7	9.4	2	**9.82**
Physical Server 1 & 2 - Switch	0.3	0.7	9.82	2	**10.24**
DB Server & Backup Server	1.3	0.6	9	3	**11.34**
Customers Data	2	0.7	12	3	**14.1**
Internal Data	2	0.7	12	3	**14.1**

we compute the maximal value. Finally, we multiply the 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.

In the Table 2 we can see the example of adjusted risk values of four assets. 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 just +0.21 point. The second asset has medium dependency and medium RV, the original risk will be adjusted by +1.05 points. The third asset has also medium dependency, but one of its component weight values has a large value, so the adjustment value raises significantly in comparison to the last case, it is adjusted by +3.00. Finally, we have an asset with high dependency and high RV, so the adjustment in this case will be +5.76 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. Values of the physical connections are in light blue boxes, values of the logical connections are in light green boxes. In Table 3 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. The risk value of physical servers is added gradually, since they depend on three entities.

Adjusted values in the whole organization model are listed in Figure 4. Main and Secondary buildings are the only two entities that do not depend on any other entity, therefore their risk values remains the same. Minimal adjustments were made to Router 1 and Switch, after considering dependencies they have

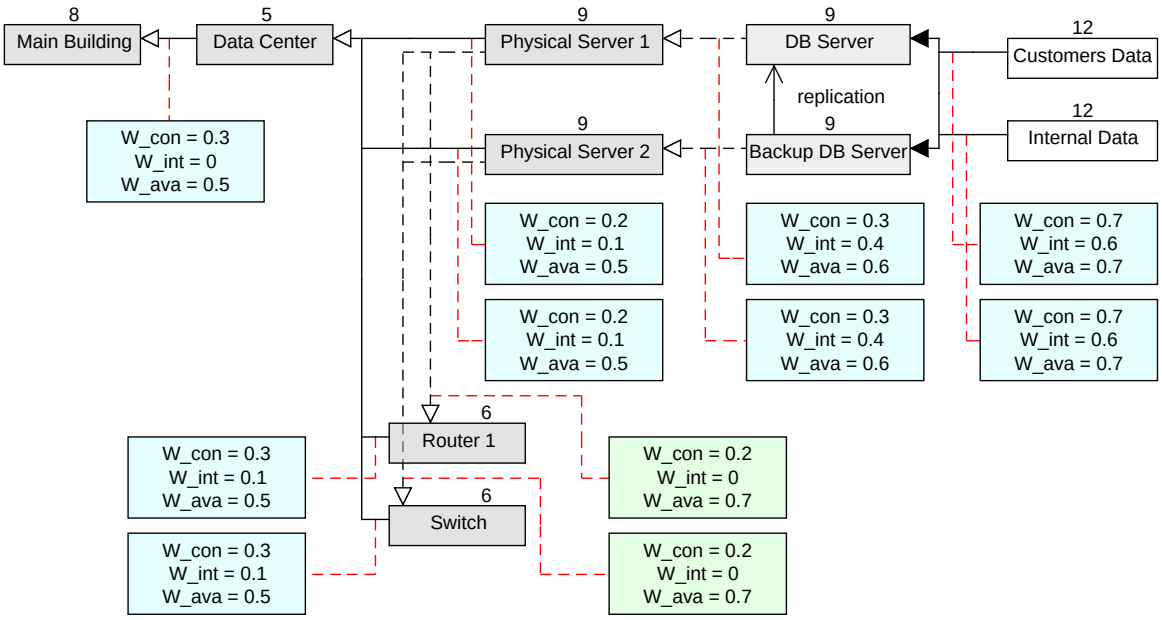

Figure 3: Dependency component weight values.

+0.45 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.

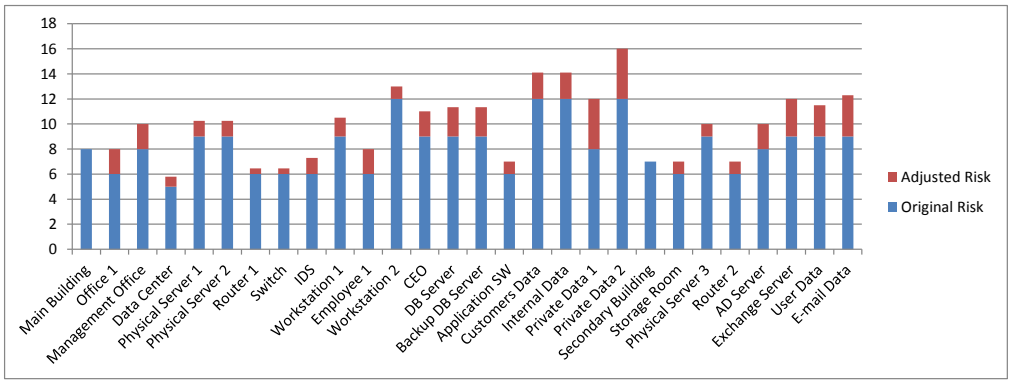

Figure 4: Adjusted risks in the whole model.

4 Discussion

We presented an approach for identification of dependencies between assets in the process of information security risk management. This approach can be inherited in a complex evaluation system in order to improve asset valuation by examining relationships among assets.

The assignment of dependency values is carried out between every two assets that have direct relation in the hierarchy. The overall value has three component values - confidentiality, integrity and availability,

each of them can hold values from interval [0,1]. Beginning with the top-level entity, dependencies are then distributed further so that the leaves in a tree-type hierarchy are influenced by all the other assets in the chain of dependence.

There are very few works examining dependencies between assets. Comparing our approach to [11] we find our method less complicated to use, but still sophisticated enough to provide quality results. Based on previous experience, risk analysts usually tend to employ simple methods providing fast and unbiased results [16, 5]. Our method can be easily inserted into risk management process in an organization and it will improve the overall outcomes produced by the evaluation.

If we analyze dependency analysis provided in [14], it is far too straightforward to provide sufficiently detailed results. Besides taking only the maximum of the importances of previous entities in the chain, it needs to adjust the raw results by security analyst. Our method is deterministic - the outcomes are evaluated strictly with respect to provided inputs.

5 Conclusions

Asset dependencies should be taken into consideration when performing risk analysis in an organization. Even the ISO/IEC 27005:2011 standard [7] recommends to analyze assets from this perspective and reflect these results into the risk management processes. There is a lack of works trying to formalize this problem, so usually it depends on risk analyst how he deals with it.

In this paper we proposed an approach of defining asset dependencies and we provided an example on simplified organization model. Dependencies are assigned to the relations between each two assets in the hierarchic structure and we examine them from the confidentiality, integrity and availability point of view. Our approach can differentiate between simple connections, dependencies on more than one entity and with redundant entities. We also consider differences between physical and logical connections. Based on these conditions, the final risk value can be adjusted in a positive or negative way.

The purpose of our method is to provide easy to use tool that can be encompassed in the risk analysis process without affecting other sub-processes. Our goal is to implement a complex risk management evaluation method that could be used in order to simplify and automate all the related actions.

References

[1] *NIST Special Publication 800-39 Managing Information Security Risk - Organization, Mission, and Information System View*. NIST, 2011.

[2] J. Bhattacharjee, A. Sengupta, C. Mazumdar, and M. S. Barik. A two-phase quantitative methodology for enterprise information security risk analysis. In *Proc. of the 2012 CUBE International Information Technology Conference (CUBE'12), Pune, India*, pages 809–815. ACM, September 2012.

[3] B. Blakley, E. McDermott, and D. Geer. Information security is information risk management. In *Proc. of the 4th workshop on New security paradigms (NSPW '01), Cloudcroft, New Mexico, USA*, pages 97–104. ACM, September 2001.

[4] J. Breier and F. Schindler. Assets dependencies model in information security risk management. In *Proc. of the 2nd Asian Conference on Availability, Reliability and Security (AsiaARES'14), Bali, Indonesia, LNCS*, volume 8407, pages 405–412. Springer-Verlag, April 2014.

[5] S. N. Foley. Security risk management using internal controls. In *Proc. of the 1st ACM workshop on Information security governance (WISG'09), Chicago, Illinois, USA*, pages 59–64. ACM, November 2009.

[6] E. Humphreys. *Information security risk management: Handbook for ISO/IEC 27001*. BSI, 2010.

[7] ISO. *ISO/IEC Std. ISO 27005:2011, Information technology - Security techniques - Information security risk management*. ISO, 2011.

[8] ISO. *ISO/IEC Std. ISO 27001:2005, Information technology - Security techniques - Information security management systems - Requirements*. ISO, 2013.

[9] A. Leitner and I. Schaumuller-Bichl. ARiMA - a new approach to implement ISO/IEC 27005. In *Proc. of the 2nd International Logistics and Industrial Informatics (LINDI'09), Linz, Austria*, pages 1–6. IEEE, September 2009.

[10] N. Liu, J. Zhang, and X. Wu. Asset analysis of risk assessment for IEC 61850-based power control systems part i: Methodology. *Power Delivery, IEEE Transactions on*, 26(2):869–875, February 2011.

[11] I. Loloei, H. Shahriari, and A. Sadeghi. A model for asset valuation in security risk analysis regarding assets' dependencies. In *Proc. of the 20th Iranian Conference on Electrical Engineering (ICEE'12), Tehran, Iran*, pages 763–768. IEEE, August 2012.

[12] J. Mayer and L. L. Fagundes. A model to assess the maturity level of the risk management process in information security. In *Proc. of the 11th IFIP/IEEE International Symposium on Integrated Network Management-Workshops (IM'09), Long Island, New York, USA.*, pages 61–70. IEEE, June 2009.

[13] G. Stoneburner, A. Goguen, and A. Feringa. *NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems*. NIST, 2002.

[14] B. Suh and I. Han. The is risk analysis based on a business model. *Information & Management*, 41(2), December 2003.

[15] U. Tatar and B. Karabacak. An hierarchical asset valuation method for information security risk analysis. In *Proc. of the Internatinal Conference on Information Society (i-Society'12), London, UK*, pages 286–291. IEEE, June 2012.

[16] A. van Cleeff. A risk management process for consumers: the next step in information security. In *Proc. of the 13th workshop on New security paradigms (NSPW'10), Concord, Massachusetts, USA*, pages 107–114. ACM, September 2010.

[17] N. Vavoulas and C. Xenakis. A quantitative risk analysis approach for deliberate threats. In *Proc. of the 6th International workshop on Critical information infrastructures security (CRITIS'11), Lucerne, Switzerland, LNCS*, pages 13–25. Springer-Verlag, September 2011.

[18] R. Williams, G. Pandelios, and S. Behrens. *Software Risk Evaluation (SRE) method description (version 2.0)*. Carnegie Mellon University, Software Engineering Institute, 1999.

Author Biography

Jakub Breier received his Bachelor degree in informatics at the Slovak University of Technology, Faculty of Informatics and Information Technologies (FIIT STU) in 2008. He continued with his studies at the Masaryk University in Brno, Faculty of Informatics (FI MU), where he received his Master degree in security of information technologies. He received his PhD degree at FIIT STU in the field of Applied Informatics. His research interests are in the area of security controls and standards, cryptography and side-channel attacks.