Franklin University
FUSE (Franklin University Scholarly Exchange)

Faculty and Staff Scholarship

2012

# An Hierarchical Asset Valuation Method for Information Security Risk Analysis

Bilge Karabacak
*Franklin University*, bilge.karabacak@franklin.edu

Unal Tatar

Follow this and additional works at: https://fuse.franklin.edu/facstaff-pub

 Part of the Information Security Commons

## Recommended Citation

Karabacak, B., & Tatar, U. (2012). An Hierarchical Asset Valuation Method for Information Security Risk Analysis. *International Conference on Information Society* Retrieved from https://fuse.franklin.edu/facstaff-pub/42

This Conference Proceeding is brought to you for free and open access by FUSE (Franklin University Scholarly Exchange). It has been accepted for inclusion in Faculty and Staff Scholarship by an authorized administrator of FUSE (Franklin University Scholarly Exchange). For more information, please contact karen.caputo@franklin.edu.

# *An Hierarchical Asset Valuation Method for Information Security Risk Analysis*

Ünal Tatar
TUBITAK-BILGEM-UEKAE Information Systems Security Division Ankara, Turkey
tatar@uekae.tubitak.gov.tr

Bilge Karabacak
TUBITAK-BILGEM-UEKAE Information Systems Security Division Ankara, Turkey
bilge@uekae.tubitak.gov.tr

*Abstract*— **The widespread use of information technology transforms businesses continuously and rapidly. Information technology introduces new threats to organizations as well. Risk analysis is an important tool in order to make correct decisions and to deal with cyber threats. Identification and valuation of assets is a crucial process that must be performed in risk analyses. Without properly identified and valued assets, the results of risk analyses lead to wrong decisions. Wrong decisions on information security may directly affect corresponding business processes. There are some finished and applied methods in literature for asset identification and valuation; however these methods are complicated and are not suitable for practical information security management projects. In this paper, a hierarchy based asset valuation method is proposed. Our method is intended to minimize the common mistakes that were done during Information Security Management Projects. The application of the method has not been performed yet; however it is thought that it can ease the processes and reduce the number of errors.**

***Keywords- Information security risk analysis, asset valuation***

## I. INTRODUCTION

Information technologies evolved from stand alone batch applications to modern interconnected mobile systems. This evolution resulted in the widespread use of information technologies by all types of businesses. Information technologies have become an inseparable part of doing business today. Two decades ago, most of the business processes were paper based in almost every organization; however almost every process is dependent on information technologies today. Therefore, while information systems started as tools for improving operational efficiency, later on, they acquired an indispensable role for the organization's survival [1], [2].

Parallel to the common use of information systems in organizations, threats and attacks on the information systems also increased rapidly. Rapid change of computing environments provides many opportunities for attackers. For instance, widespread use of distributed communication systems gives attackers the chance of hiding themselves after breaking into a system remotely [3]. Mobile equipment attract hackers' attention because of their widespread use. Mobile systems are also vulnerable to attacks [4].

Number of security incidents and threats rises day by day [4]. Since most of the business operations depend on information technologies, a threat to the information technologies means a threat to the business itself. Bulgurcu et al. state that some possible results of the information security incidents could be loss of credibility and monetary damage [5]. Farahmand et al. believes that impact on the business is a good indicator to determine the cost of a computer security incident [6]. Other than the financial impact, security incidents may have effects on intangibles such as:

- The brand image, public reputation and goodwill in the market place,
- The financial value of business transactions,
- Public and customer confidence in the accuracy of business transactions,
- Public and customer confidence in the fraud-resistance of business transactions,
- The ability to maintain revenue cash flow in a timely manner,
- The ability to resolve disputes beyond reasonable doubt,
- The ability to meet the requirements of regulators [6].

Since information technologies are more critical than ever and organizations heavily rely on information systems, the responsibility of protecting these systems belongs to senior level management rather than the head of information processing department [7]. Information security has become one of the top priorities of senior level management [5]. In ISO/IEC 27001:2005, management shows its commitment to the organization's information security by deciding the criteria for accepting risks and the acceptable level of risk [8].

Information security aims to provide controls in order to mitigate risks that affect the information of organizations. Critically, there is a danger of spending money on risks that may not be really dangerous, while ignoring others that may be serious [9]. The top level management, which is the decision making body and responsible for choosing the security measures for information security risks, needs a practical guidance for choosing necessary risk reduction controls to

This work is sponsored by The Turkish Ministry of Development under the Information Systems Security Program for Government

obtain an acceptable level of security. Risk management techniques provide assistance to organizations for identifying threats and select cost-effective security measures to minimize the total expected cost of losses [3], [10].

## II. INFORMATION SECURITY RISK ANALYSIS

Although they have different meanings in literature, risk analysis, risk assessment and sometimes risk management are used interchangeably. We will use risk analysis in the remaining part of the paper. Risk is defined as a probabilistic function of a threat successfully attacking an asset through a specific vulnerability [3], [10-13].

As shown in Fig. 1, asset value, asset vulnerability and probability of the realization of a threat forms the risk and all these factors have a positive effect on risk.

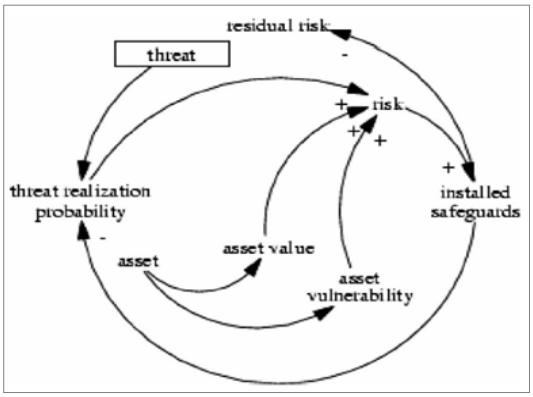


Figure 1. Risk, threat, vulnerability and asset relationship [11]

The risk function given in (1) has three variables: asset, vulnerability and threat. The first input of the risk function, asset, is defined as anything that has value to the organization in ISO/IEC 27001:2005. Determining the value of an asset is a crucial part of risk analysis.

$$\text{Risk} = f(\text{asset}, \text{vulnerability}, \text{threat}) \quad (1)$$

Vulnerability is a defect in an asset that may be used by a threat to attack an information system. Software and hardware companies try to adapt the rapid pace of change at information technologies for sustaining their competitiveness; however rapid change of technology may cause neglecting security requirements which slow down the production process. Every day new technologies are introduced and attackers find a vulnerability to exploit it after a while. For a successful risk analysis, security analyst should reach and exchange information about new technologies, products, threats, or vulnerabilities and keep themselves up to date.

Threats to information systems may impact confidentiality, integrity and/or availability of an asset. Threats may operate in several ways such as destruction (the asset is not recoverable), modification (changing the representation of an asset), disclosure (violation of need-to-know), and denial of service (resources are unavailable to authorized users) [3]. Common threats for information security are listed below [14].

1) Act of Human Error or Failure (accidents, employee mistakes)
2) Compromises to Intellectual Property (piracy, copyright infringement)
3) Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection)
4) Deliberate Acts of Information Extortion (blackmail of information disclosure)
5) Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)
6) Deliberate Acts of Theft (illegal confiscation of equipment or information)
7) Deliberate Software Attacks (viruses, worms, macros, denial of service)
8) Forces of Nature (fire, flood, earthquake, lightning)
9) Quality of Service Deviations from Service Providers (power and WAN service issues)
10) Technical Hardware Failures or Errors (equipment failure)
11) Technical Software Failures or Errors (bugs, code problems, unknown loopholes)
12) Technological Obsolescence (antiquated or outdated technologies)

Risk analysis methods are divided into two major groups as qualitative and quantitative methods. Quantitative risk analysis methods use mathematical tools (e.g. Bayesian networks, fuzzy logic) to assess the risk [12]. Quantitative methods try to calculate annualized loss expectancy in monetary value for each threat and find the cost of a possible damage [1], [3]. Courtney method, Livemore Risk Analysis Methodology (LRAM), Information Security Risk Analysis Method (ISRAM), and ALE using program evaluation review technique (PERT) are instances of quantitative risk analysis methods [1], [7]. Quantitative methods require a solid mathematical background to assess information security risks and implementation of these methods requires more time and effort than qualitative methods [3], [12].

Qualitative risk analysis methods claim that using monetary values to express a possible consequence of a threat is not a good method [1]. Generally, these methods are based on judgments and perceptions of the security expert that conducts the risk analysis and make use of several techniques such as questionnaires, scenario analysis, and fuzzy metrics to assess the suitability of the safeguards against the identified threats [1], [3].

Neither of these methods have been proven superior to the other. An organization can choose any of these methods that is suitable for it, for instance qualitative methods are suggested for risk analysis of public organizations [12]. Advantages and disadvantages of these two types of methods are summarized in Table 1 [1], [6].

TABLE I. ADVANTAGES AND DISADVANTAGES OF RISK ANALYSIS METHODS

| Quantitative methods | Qualitative methods |
|---|---|
| ***Advantages*** | |
| Applicability to all assets | Simple risk calculation |
| Mathematical foundation | Usefulness when asset value is irrelevant or unknowable |
| Using a management specific language (Support cost benefit decision) | Less time consuming |
| Accuracy tends to increase over time as the organization builds historic record of data while gaining experience. | Easier to involve people who are not experts on security or computers. |
| ***Disadvantages*** | |
| Inappropriateness of monetary asset value | Coarse granularity |
| Inappropriateness of general statistics | Inability of cost benefit decision |
| Time consuming, requires much preliminary work | Subjective results, depend on quality of risk management team |

Whatever methodology is used in risk analysis, there are desired properties of a risk analysis method. The essential properties of a risk analysis method are listed below [10].

- Common acceptance by all related parties (e.g. management, users, IT department)
- Handling new technologies, threats and vulnerabilities
- Logically sound
- Repeatable
- Delivering optimum protection for the cost
- Being open to continuing evaluation from all parties
- Being accompanied by clear documentation
- Being cyclical, repeated periodically.

Up to now, we examined two of the inputs of the risk analysis function, which are vulnerability and threat. The third input, asset, is detailed in the next section of the paper.

## III. THE IDENTIFICATION AND VALUATION OF ASSETS

The identification and valuation of assets is a crucial step in order to have an objective, repeatable and logically sound risk analysis process. The asset identification and valuation process also affects the comprehensiveness and effectiveness of the eventual risk analysis process. Therefore, asset identification and valuation is not a straightforward task. Identification and valuation of information assets gets more difficult when an asset is intangible such as reputation of the organization. There are not many studies on asset valuation methods for information security risk analysis processes. We summarize the academic works on asset valuation in the remaining part of the section.

Oscarson and Karlsson propose a national model for information classification. Their model is based on two aspects: the information system security aspect and the levels / types of seriousness. In the information systems security aspect, there are two documents for definitions of confidentiality, integrity and availability. These documents are ISO 27000 series (ISO/IEC 27001:2005 and ISO/IEC 27002:2005) which are compulsory for governmental authorities in Sweden and SIS Handbook 550 Terminologi för Informationssäkerhet (in Swedish, Terminology for Information Security). These documents say nothing about level and types of seriousness which is the other dimension of the classification. Oscarson and Karlsson define three levels for this aspect: moderate, significant and serious. According to the suggested model, the information aspect is classified and valued for these two dimensions [15].

Vidalis identifies the value of information assets according to confidentiality, integrity and availability. Value of an asset is defined as follows; “An exploitation of an asset ‘A’ can cause a loss of confidentiality ‘Co’, a breach of integrity ‘In’ or a loss of availability ‘Av’. The value ‘V’ of each asset is the cost of restoring or repairing the sum of the above qualities in their previous state.”. ‘Co’ is the monetary value to restore confidentiality, ‘In’ is the monetary value to restore integrity, ‘Av’ is the monetary value to restore availability, and ‘V’ the monetary value of an asset. The definition is formulated in (2) [16].

$$V = f(Co) + f(In) + f(Av) \quad (2)$$

Engelsman’s study on valuation of information assets is in a wider perspective than information security. Information valuation depends on four dimensions in Engelsman’s model: defining information assets, identifying the audience for the valuation, determination of the context of the valuation and identifying what economic attributes of information to include in the valuation. In his four stage model, after the first step of identifying assets, the external and internal audiences for information assets are identified. External audiences are useful for determining the contribution of information to the overall value of an organization and valuation for an internal audience shows the value of the information to encourage better use of the information such as improved decision making. The third stage is determining the context of valuation e.g. valuation of information for security risk management and valuation of information for information life cycle management. The forth and last stage is valuation of information using an existing model or coming up with a model that is suitable for this specific valuation context [17].

Caralli et al. from Carnegie Mellon University Software Engineering Institute, prepared a technical report to introduce the next generation of the Operationally Critical Threat, Asset,

and Vulnerability Evaluation (OCTAVE) methodology, OCTAVE Allegro. In their report, they propose a framework to develop an information asset profile. Development of an information asset profile is composed of eight steps. First step is identifying the information assets through brainstorming on information assets that are used in day-to-day work processes and other assets that are closely related to these assets. Second step is focusing on the few critical assets which are critical to accomplishing goals and achieving the organization's mission and those that are important because of such factors as regulatory compliance. Remaining steps are performed as a completion of a worksheet for each asset. In the third step, the name of the critical asset is written on the worksheet. In forth step, rationale for the selection of the asset as a critical asset is reported. In the fifth step the agreed-upon description of the information asset is determined. The sixth step is defining the owners of the asset. The seventh step is identifying security requirements (confidentiality, integrity, availability, and other) for this asset. At the last and eighth step, selection of the most important security requirement is performed [18].

Grimaila and Fortson use information valuation in the cyber damage assessment process of military systems. Information classification is a baseline valuation of an asset and to complete the valuation process the contextual value of the information should be determined. Contextual value of an information asset depends on how much the asset supports the organizational mission. According to Grimaila and Fortson, most of the existing models focus on economic metrics; however the intangible value of an information asset is used more frequently in a military context compared to economic value. In the information valuation method, first step is the classification of information. The second step is to identify the contextual value of the information which is the most important component in information asset valuation. Contextual value is composed of three factors: mission binding, age, and state. Mission binding is about how related the information asset is to the organization's mission. If the information asset has a critical function for the organization's mission, it will possess a relatively high value. The second factor, age, is about change in the value of the information asset and its relation with the organization's mission during its lifecycle. The third and last factor of contextual value is the state in which the value of the information asset is determined in terms of confidentiality, integrity and availability [19].

## IV. THE PROPOSED METHOD

Our method is proposed in order to minimize the common mistakes that were made during Information Security Management Projects that were performed for public organizations of Turkey.

According to Karabacak and Ozkan [?], during the identification and valuation of assets, authors realized that only tangible assets like hardware and software were listed in almost all of these eight projects. For the "information" security projects, the most crucial assets are "information" assets, which are intangible. Without taking "information" into consideration, the asset inventory cannot be established reliably and the values of assets cannot be determined correctly. The vulnerabilities in assets and the threats that exploit these vulnerabilities are determined by using asset inventory. Thus, a tangible asset inventory would cause an incomplete risk analysis focusing only on technical dimensions of information security disregarding the social and non-technical dimensions. The inevitable consequence of this problem is to assign wrong asset values to hardware and software; because the information that is processed by hardware and software is not determined [12].

In order to recover from this mistake, a practical asset valuation method is proposed. There are two important contributions of the proposed method. First of all, it helps risk analysts to list information assets completely. Secondly, it helps the values of hardware and software to be determined correctly. Our proposed method is presented in Fig. 2. As with other methods, firstly assets are identified by using a top-down approach (the left arrow in Fig. 2). After assets are identified, the valuation of assets are performed by using a bottom-up approach (the right arrow in Fig. 2).

First of all, hardware assets are identified, because they are the most tangible assets, so they can easily be determined without much effort. After hardware assets are identified, the software assets that are run on each hardware asset are identified. After software assets are identified, the information assets that are processed by software assets are identified.

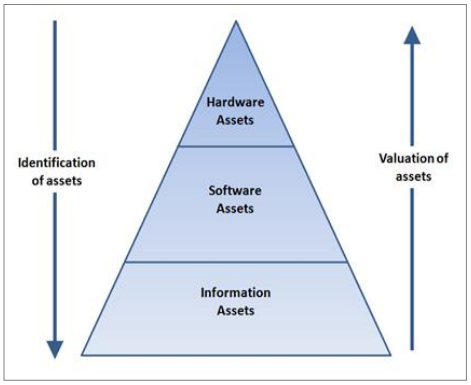


Figure 2. Asset pyramid showing asset identification and asset valuation processes

After assets are identified, the values of assets are determined. The result of asset identification and valuation processes should be presented in asset tables. The asset tables - when filled with asset names and values- form the asset inventory which is a basic component for Information Security Management projects. The asset tables may contain not only asset names and values but also other information like serial numbers, owner, location etc. In our proposed method, the templates of asset tables for hardware, software and information assets are shown in Table 2, Table 3 and Table 4 respectively. Note that, there are some differences among these tables.

The template table for hardware assets is shown in Table 2. An important point is that, the physical location of a hardware

asset is included in order not to forget any hardware asset. In our proposed method, only hardware assets that processes information are written in the asset table. As an example, mouse and keyboards are not written in the inventory.

TABLE II. THE ASSET TABLE TEMPLATE FOR HARDWARE ASSETS

| Serial no | Hardware Name | Owner / Custodian | Physical Location | Confidentiality value | Integrity value | Availability value |
|---|---|---|---|---|---|---|
| H1 | Fileserver | Paul | Server room | 5 | 5 | 5 |

The template table for software assets is shown in Table 3. The "processing hardware" column is used in order to control whether all software assets are written in the inventory.

TABLE III. THE ASSET TABLE TEMPLATE FOR S ASSETS

| Serial no | Software Name | Owner / Custodian | Processing Hardware | Confidentiality value | Integrity value | Availability value |
|---|---|---|---|---|---|---|
| S1 | Operating system | Paul | H1 | 3 | 3 | 5 |
| S2 | Encryption software | Paul | H1 | 5 | 5 | 4 |

The template table for information assets is shown in Table 4. The "processing software" column is used in order to control whether all information assets are written in the inventory.

TABLE IV. THE ASSET TABLE TEMPLATE FOR INFORMATION ASSETS

| Serial no | Infor-mation Name | Owner / Custodian | Processing Software | Confidentiality value | Integrity value | Availability value |
|---|---|---|---|---|---|---|
| I1 | Personal data | Ann | S2 | 4 | 4 | 4 |
| I2 | Salary data | Ann | S2 | 5 | 5 | 2 |

Note that all tables include minimum set of columns for demonstration purposes. The other columns like "explanation" and "license" can be added for real information security projects.

After hardware, software and information assets are determined, the asset values are determined for all types of assets. The work done in the asset valuation process is to fill the last three columns of the templates. Asset valuation is based on three values, confidentiality, integrity and availability that are the tripod of information security. Asset valuation is a bottom-up process as it is presented by the right arrow in Fig. 2.

The confidentiality, integrity and availability values of information are directly related with the nature of the information. Also, information is the most crucial asset for organizations especially in the context of "Information" Security Management Projects. Those are the most important reasons why a bottom-up approach is adopted. The Confidentiality, Integrity and Availability CIA values of software are directly related with the Confidentiality, Integrity and Availability values of information that is processed by that software. In the same manner, the Confidentiality, Integrity and Availability values of hardware are directly related with the Confidentiality, Integrity and Availability values of the software that is processed by that hardware. The value of software and hardware is directly proportional to the value of processed information. The monetary value of hardware can be negligible compared to the value of information processed by that hardware.

If there is a number of software in a specific hardware, the highest Confidentiality, Integrity and Availability values assigned to the software assets are taken into account when assigning Confidentiality, Integrity and Availability values to the hardware. The same condition is valid for determining Confidentiality, Integrity and Availability values of specific software, if the software in question processes more than one type of information.

As an example, Table 2, Table 3 and Table 4 is filled with fictitious asset information. First of all, hardware assets are identified and the first four columns of Table-2 are filled. Secondly, software assets are identified and the first four columns of Table-3 are filled. Thirdly, information assets are identified and the first four columns of Table-4 are filled. The top-down approach (left arrow at Fig. 2) is finished at this point.

After all asset types are identified, bottom-up approach (right arrow at Fig. 2) starts in order to determine asset values. Firstly, information asset values are determined and the values are written at the last three columns of Table-4. For the "information security" context, it is easier to assign Confidentiality, Integrity and Availability values to information assets compared to hardware and software assets, because information assets are not complicated, they are plain and elementary. Secondly, software asset values are determined by using the values of information assets in Table-4. It can be seen from Table-4 that personal data and salary data are processed by encryption software. Therefore, Confidentiality, Integrity and Availability values of encryption software is determined by using Confidentiality, Integrity and Availability values of processed information, namely personal data and salary data. For instance, the confidentiality value of encryption software is the highest of confidentiality values of the two information assets, personal data and salary data. The same rule applies to integrity and availability values. These highest values are underlined in Table-4. Thirdly, hardware asset values are determined. This is performed by using the software asset table, Table-3. As it can be seen from Table-3, both the operating system and encryption software are processed by the fileserver. Therefore, the Confidentiality, Integrity and Availability values of these software are used in order to determine the Confidentiality, Integrity and Availability values of the fileserver hardware. The underlined values in Table-3 are also the Confidentiality, Integrity and Availability values of the fileserver hardware. After hardware asset values are determined, the bottom-up approach finishes and the asset inventory is created.

## V. DISCUSSION AND CONCLUSION

First of all, our method has some drawbacks. It only deals with digital assets. As an example, it does not cover printed books. The assets that are not hardware, software or digital information should be considered separately. Our method can

be used effectively in risk analysis processes where mostly information technologies are used.

Risk analysts should be cautious while dealing with hardware such as hard disks. There is no explicit software (e.g. operating systems, application programs) in hard disks. They run special software called firmware; but firmware is not usually considered as a standalone asset. It is considered with hardware as a whole. Therefore, risk analysts should skip the middle layer of the asset valuation pyramid and should directly identify the information assets within hard disks.

An important question is: "Which values among Confidentiality, Integrity and Availability should be taken into account during the risk analysis process?" Is using arithmetic mean a good idea? For our proposed method, the answer is related to the type of risk involved. If the risk is related with the availability of information, the availability value should be taken into account. As an example, a flood may affect the availability of a server, but it does not affect confidentiality and integrity. So, when evaluating the risk, the availability value of related hardware should be used but not confidentiality and integrity values.

We think that our proposed method can ease the asset valuation and risk analysis processes. Our practical approach can help organizations that try to improve their information security procedures. Our next step will be to apply our method in information security projects in the Turkish Public Sector Organizations and to share the results with academia.

## REFERENCES


[1] Suh, B., Han, I.: The IS Risk Analysis Based on a Business Model. Information & Management. Vol. 41, No. 2, 149-158 (2003)

[2] Doherty, N. F., Anastasakis, L., Fulford, H.: The Information Security Policy Unpacked: A Critical Study of the Content of University Policies. International Journal of Information Management. Vol. 29, No. 6, 449-457 (2009)

[3] Wilson, J.L., Turban, E., Zviran, M.: Information Systems Security: A Managerial Perspective. International Journal of Information Management. Vol. 12, No. 2, 105-119 (1992)

[4] Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., Blackbird, J., Low, M.K., Mazurek, D., McKinney, D., Wood, P.: Symantec Internet Security Threat Report Trends for 2010. Symantec (2011)

[5] Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. Vol. 34, No. 3, 523--548 (2010)

[6] Farahmand, F., Navathe, S. B., Sharp, G. P., Enslow, P. H. A Management Perspective on Risk of Security Threats to Information Systems. Information Technology and Management. Vol. 6, No. 2-3, 203-225 (2005)

[7] Karabacak, B., Sogukpinar, I.: ISRAM: Information Security Risk Analysis Method. Computers & Security. Vol. 24, No. 2, 147-159 (2005)

[8] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC): ISO/IEC 27001:2005, Information Technology -- Security Techniques -- Information Security Management Systems - Requirements. Edition 1 (2005)

[9] Solms, B. von, Solms, R. von: The 10 Deadly Sins of Information Security Management. Computers & Security. Vol. 23, No. 5, 371-376 (2004)

[10] Rainer Jr., R.K., Snyder, C.A., Carr, H.H.: Risk Analysis for Information Technology. Journal of Management Information Systems. Vol. 8, No.1, 129-147 (1991)

[11] Trček, D., Trobec, R., Pavesic, N., Tasic, J.F.: Information Systems Security and Human Behavior. Behaviour & Information Technology. Vol. 26, No. 2, 113- 118 (2007)

[12] Ozkan, S., Karabacak, B.: Collaborative Risk Method for Information Security Management Practices: A Case Context within Turkey. International Journal of Information Management. Vol. 30, No. 6, 567-572 (2010)

[13] Chen., P., Kataria, G., Krishnan, R.: Correlated Failures, Diversification, and Information Security Risk Management. MIS Quarterly. Vol. 35, No. 2, 397-422 (2011)

[14] Whitman, M.E.: In Defense of the Realm: Understanding the Threats to Information Security. International Journal of Information Management. Vol. 24, No. 1, 43-57 (2004)

[15] Oscarson, P., Karlsson, F.: A National Model for Information Classification, Association of Information Systems. In: SIGSEC Workshop on Information Security & Privacy, Phoenix, AZ, USA (2009)

[16] Vidalis, S.: Calculating the Value of Information Assets, Newport Business School Working Paper Series, Vol. 1, No. 2-3 (2007)

[17] Engelsman, W.: Information Assets and Their Value. In: 6th Twente Student Conference on IT, Enschede, Netherlands (2007)

[18] Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R.: Introducing Octave Allegro: Improving the Information Security Risk Assessment Process, Technical Report, SEI/CMU (2007)

[19] Grimaila, M.R. Fortson, L.W.: Towards an Information Asset-Based Defensive Cyber Damage Assessment Process. In: IEEE Symposium on Computational Intelligence in Security and Defense Applications, pp. 206-212 (2007)