OmniaScience

Journal of Industrial Engineering and Management
JIEM, 2016 – 9(4): 964-977 – Online ISSN: 2013-0953 – Print ISSN: 2013-8423
http://dx.doi.org/10.3926/jiem.2032

Information Security Risk Management and Incompatible Parts of Organization

Elham Talabeigi[1], Seyyed Gholamreza Jalali Naeeini[2]

[1]*International University of Chabahar (Iran)*
[2]*Iran University of Science and Technology (Iran)*

etalabeigi2@gmail.com, *sgjalali@iust.ac.ir*

Received: July 2016
Accepted: September 2016

Abstract:

Purpose: we prepared a questionnaire to evaluate Incompatible parts and also risk management in University of Science and Technology E-Learning Center and studying the Incompatible parts impacts on utility of organization.

Design/methodology/approach: By using coalitional game theory we present a new model to recognize the degrees of incompatibility among independent divisions of an organization with dependent security assets. Based on positive and negative interdependencies in the parts, the model provides how the organization can decrease the security risks through non-cooperation rather than cooperation. we implement the proposed model of this paper by analyzing the data which have been provided by questionnaires from different three managers' ideas of Iran University of Science and Technology E-Learning Center located in Iran University of Science and Technology, Tehran, Iran.

Findings: In general, by collecting data and analyzing them, the survey showed that Incompatible parts of organizations have negative impacts on utility of organization risk management process. Furthermore, it adds values to other organizations and provides the best practices in planning, developing, implementing and monitoring risk management in organizations.

Research limitations/implications: Since Information security and also Risk Management are still areas which need to improve in some Iranian universities, we couldn't consider them in our analysis. On the other hand, due to questionnaire limitation, the study's sample size is 1. This size may be considered large for our statistical analysis.

Originality/value: The main contribution of this paper is to propose a model for non-cooperation among a number of divisions in an organization and using risk management factors.

Keywords: coalitional game theory, incompatible parts, risk management, security

1. Introduction and Literature Review

Today, the organizations and systems have been in an environment full of challenge and transformation. So, in this dynamic environment, organizations are needed to pace with environmental changes and make a good decision. When deciding must be considered probability Risks that can have effect on decision results, these areas discussed in the risk management. Decisions in the field of risk management need to consider risk management rules and procedures.

Chai, Kim and Raghav-Rao (2011), stated that in the information society, it is important for firms to manage their core information resources securely. Managers to achieve this objectives should be emphasized on the information security, break the security boundaries defined for organization and all the factors threaten encompass the information. In addition, the costs of implementing an efficient security policy are important. So, a comprehensive plan and strategy is needed that dealing with all cases threat. Arshad, Mohamed and Mansor (2009), showed that the organizational structure and risk management strategies, organization strategies, technology and knowledge organization are placed in a row. Therefore, a mechanism to create a strategic risk management technique in project risk management and control system information is needed. Moreover, risk management techniques, risk, uncertainty, and mistakes can potentially be acknowledged and immediately be dealt with rather than ignore it and hid.

Workman (2007), demonstrated that there are many threats to the integrity, confidentiality, and availability of information maintained by organizational systems. Key issues related to internal threats have for information security: nature and honesty in corporate and cultural factors, social and economic changes considered and stating that the security risk for legal access to facilities, information, knowledge organization and location of assets, should be considered to reduce the threats, therefor methods of

prevention are better from methods of reactive. Colwill (2009), reported that in some cases internal security breach can be caused by human error.

Dlamini, Eloff and Eloff (2009), stated that information security vulnerabilities and associated problems have costly ramifications. It is therefore critical that securing information and infrastructures should not be considered in fear of inevitable attacks, but in preparation for the uncertain future. Gordon, Loeb and Tseng (2009) demonstrated that effects of proper risk management life cycle impact on the organization such as increasing efficiency and effectiveness, reduce costs, identify threats to the system and so on. Yildirim, Akalp, Aytac and Bayram (2010), showed that for information security in small and medium companies, factors such as security, environmental, physical, organizational and personnel were asked to consider and stated that these parameters need to improve communications and operations management and security policies to be better.

Awareness of the risks in their organizations is growing and organizations must learn how to manage security risk. Today, risk management is a component of a strong program of information security in an organization. Risk management in this area is faced with the opportunities and challenges in research. In recent years, the study of the risk management framework has been little analytical.

a) Related work on the security risk management

Threat trees and attack trees are graphical notations that have evolved from fault trees, Howard and LeBlanc (2002) using threat trees and Schechter (2004) applying attack trees illustrated attackers' goals together with possible ways to reach these goals.. The attacker's main goal is depicted as the root of the tree and the steps to reach this goal are broken down into sub-goals of the attack through "AND" and "OR" relationships. Threat trees and attack trees have been applied in several ways to assess security. Howard and LeBlanc (2002) suggested that the threat trees should be used to rank the threats is terms of risk. Karabacak and Sogukpinar (2005) showed that Information Security Risk Analysis Method (ISRAM) in a similar way guide the analyst to assess probabilities for security incidents to occur and to assess the potential consequences of these. Alberts and Dorofee (2001) stated that the same type of guidance is also provided by Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). Architectural models provide decision makers with a convenient tool to abstract and capture different aspects of information systems in diagrammatic descriptions. Hogganvik (2007) stated that meta-models like the one offered in CORAS guide the modeler to create graphical descriptions that can be used to assess risk. This type of meta-models does however not help the modeler to identify the risks which their particular architecture face, and do not provide the data needed to quantify security or risk based on the model.

Hogganvik (2007) showed that CORAS is a method specifically developed for analyzing and quantifying risk.. With guidance from CORAS's meta-model, a graphical description of the threat scenario is created and used as a support to determine if, and how, the identified risks should be treated. This is done by modeling the relationships between assets, threats, vulnerabilities, unwanted events, risks and treatments. Although risk in CORAS is defined as the product of likelihood and consequence, there is no analysis framework coupled to the meta-model and thus no algorithmic method to calculate risk based on a graphical description. There is also no description of what different types of risk treatments that should be modeled, or how risk treatments influence risks in CORAS.

These calculations, as well as the content of the CORAS diagram, must instead be assessed by the persons applying CORAS.

b) Using Game theory in Information Security

Morris (1994) stated that game theory has been successfully applied to many disciplines including economics, political science, and computer science. Game theory usually considers a multiplayer decision problem where multiple players with different objectives can compete and interact with each other. Golany, Kaplan, Marmur and Rothblum (2009), Hausken and Levitin (2009)and Liu, Wang and Camp (2008) reported that since 2001, game theory has been used as a promising scientific technique to deal with security issues. Alpcan and Basar (2004), authors presented a game-theoretic analysis of intrusion detection in access control systems. In order to establish a quantitative mathematical framework, they modeled the interaction between the attackers. The interaction between the attacker and the IDS was formulated as a non-cooperative non-zero sum game with the virtual sensor network as a third fictitious player.

Liu and Zang (2005), the authors proposed a game theoretic approach for estimating the attacker's intent, objective, and strategies (AIOS). They developed a game theoretic AIOS formalization which could capture the inherent interdependency between AIOS and defender objectives and strategies in a way that AIOS could be automatically inferred. Lima, Contreras and Feltrin (2008), have an analysis and discussion, based on cooperative game theory, for the allocation of the cost of losses to generators and demands in transmission systems. They construct a cooperative game theory model in which the players are represented by equivalent bilateral exchanges and we search for a unique loss allocation solution, the Core. Kantzavelou and Katsikas (2009) showed that notice to employees within the organization can at any time to threaten the organization system. From game theory to model the interaction of people within the organization used if that were to play in intrusion detection systems periodically is played frequently. Using games to determine how an insider in the future will interact and how an intrusion

detection system to protect the system reacts. Chatzoglou and Diamantidis (2009) on the effects of non-financial risks have discussed information technology and risks to be measured six variables are divided into operations that include the user, managing and to measure company performance, productivity and collaboration capabilities of information were considered.

Saad, Alpcan, Basar and Hjørungnes (2010), is worked on the this issue that the coalition formed to increase utility in the organization, but given that the organizations work for reasons such as lack of appropriate sections or enlarge the size of a sector when the coalition together make up, and coordination problems in these sectors cannot people with exposure to the desirability of a group seem and partnerships may not benefit the organization, studying the literature indicates the lack of detection sections is incompatible with the organization.

This paper is organized as follows. We first present the proposed methodology of our research in section 3. Section 4 explains the details validation and section 5 explains limitations on our work and finally section 6 summarizes the contribution of the paper.

2. The Proposed Framework

The main contribution of this paper is to propose a model for non-cooperation among a number of divisions in an organization and using risk management factors. We propose a model based on coalition game theory and aspect of non-cooperation in a coalition formation in a risk management. The proposed model of this paper, organization parts were considered as players and recognize incompatible divisions in the organization. These incompatible divisions reduce the utility of organization and consequently the risk in the organization is increase. No work seems to have investigated how a number of organizations or divisions in an organization can not cooperate in order to increase their vulnerabilities, and, consequently, increase their security risks.

Then under conditions of non-cooperation incompatible parts, we want to achieve high levels of risk reduction benefits that, in fact, it is the main contribution of this paper. In this way we are introduced two theories, and using these theories are identified incompatible parts, to use this theories should determine positive impact and negative impact and difference matrices. Finally, we implement the proposed model of this paper by analyzing the data which have been provided by questionnaires from different three managers' ideas of Iran University of Science and Technology E-Learning Center located in Iran University of Science and Technology, Tehran, Iran.

a) The Parameters and the Variables of the Model

Suppose an organization has a part (player), that are Shown with the i, for $i = 1, 2, \ldots, n$, let us define the parameters and the variables of the model as:

Parameter	Description
S_i	security resources, including budgets, investments, human and professional staff
t_i	threatening each section
P_{ij}	a n*n positive impact matrix
N_{ij}	a n*n negative impact matrix
$v(\{i\})$	utility of division i
$Cost(Q, C)$	a n*n cost matrix
D	a n*n difference matrix

Table 1. Parameters used

The communications between divisions in an organization have two forms:

1. Positive Communications: The communications that divisions have a positive effect on together. Show that with the matrix P_{ij}.

2. Negative Communications: The communications that divisions have a negative effect on together. Show that with the matrix N_{ij}.

$$P_{ij} = \begin{cases} 1 & if\ i = j \\ \zeta_{ij} & e_{ij} \in \mathcal{E}_p \quad i,j = 1,2,\ldots.,N \\ 0 & otherwise \end{cases} \tag{1}$$

$$N_{ij} = \begin{cases} 1 & if\ i = j \\ \lambda_{ij} & e_{ij} \in \mathcal{E}_p \quad i,j = 1,2,\ldots.,N \\ 0 & otherwise \end{cases} \tag{2}$$

The values of ζ_{ij} and λ_{ij} are between zero and one.

Utility of divisions in the organization for any division i which it tries to maximize, is calculated in this way:

$$v\{(i)\} = \left(P_{ij}\ .\ s\right)_i - \left(N_{ij}\ .\ t\right)_i \tag{3}$$

That, $s: = [s_1, s_2, \ldots, s_n]$ be the vector of security resources of all divisions for defend against security risks and $t: = [t_1, t_2, \ldots, t_n]$ be the vector of threats against vulnerabilities.

Miura-Ko, Yolken, Mitchell and Bambos (2008) proposed the linear influence model uses a matrix to represent linear dependence between resources at organization and threats at selfsame organization, and utility functions to measure the benefit to organization.

b) The Proposed Protocol

With this model, which can form parts in a larger group, indicating they are incompatible and reducing the utility in the organization. When the parts are placed in a group, matrices previously introduced, definitely get the new value. These matrices is more clearly described below:

$$\bar{P}_{ij} = \begin{cases} 1 & if\ i = j \\ W_{ij}^{p} & if\ \ i \notin S\ or\ j \notin S \quad i,j = 1,2,\ldots.,N \\ 0 \le f\left(W_{ij}^{p}\right) \le W_{ij}^{p} & if\ i,j \in S \end{cases} \tag{4}$$

For simplicity in writing:

$$0 \le f\left(W_{ij}^{p}\right) \le W_{ij}^{p} = P'_{ij}$$

$$\bar{N}_{ij} = \begin{cases} 1 & if\ i = j \\ W_{ij}^{n} & if\ \ i \notin S\ or\ j \notin S \quad i,j = 1,2,\ldots.,N \\ W_{ij}^{n} \le g(W_{ij}^{n}) \le 1 & if\ i,j \in S \end{cases} \tag{5}$$

For simplicity in writing:

$$W_{ij}^{n} \le g\left(W_{ij}^{n}\right) \le 1 = N'_{ij}$$

These incompatible divisions have the difference and difference show with the following matrix:

$$F_{ij} = \begin{cases} \chi_{ij} & if\ e_{ij} \in \mathcal{E}_F\ \ and\ \ i \neq j \\ 0 & otherwise \end{cases} \tag{6}$$

Incompatible parts placed in a group to create a cost. In addition, coalition created each increase in the size $|C|$ also provides a cost. These costs are calculated as follows:

$$Cost(D,C) = \begin{cases} \alpha.\sum_{i \in C}\sum_{j \in C} D_{ij} + \beta|C| & if\ |C| > 1 \\ 0 & otherwise \end{cases} \tag{7}$$

The parameters $\alpha \geq 0$ and $\beta \geq 0$ quantify the price of forming a coalition with $|C| > 1$ per unit friction and per unit size, respectively. Myerson (1991) proposed that characteristic function for utility in game theory terms of any coalition C will be given by:

$$v(C) = (\bar{P}.s)_c - (\bar{N}.s)_c - Cost(F, C) \quad (8)$$

That

$$(\bar{P}.s)_c := \sum_{i \in C}((\bar{P}.s)_c)_i \quad (9)$$

$$(\bar{N}.s)_c := \sum_{i \in C}((\bar{N}.s)_c)_i \quad (10)$$

While N, P, D was considered as independent variables, utility of organization served as dependent variables. The proposed problem can be modeled as a coalitional game with the players being the divisions and the function given by (8).

The following theory states necessary and sufficient condition for not merging the two coalitions that is incompatible coalition.

Theory 1: Consider two disjoint coalitions $C_1 \subseteq N$, $C_2 \subseteq N$, $C_1 \cap C_2 = \emptyset$, if the two are merged , we have in the case non-ideal:

$$v(C_1 \cup C_2) \leq v(C_1) + v(C_2) \quad (11)$$

If and only if the following conditions on the cost function is established:

$$Cost(Q, C_1 \cup C_2) - (Cost(Q, C_1) + Cost(Q, C_2)) \geq \mu \quad (12)$$

And

$$\mu := \sum_{i \in C_1}\sum_{j \in C_2}(N_{ij}t_j - P_{ij}s_j) + \sum_{i \in C_2}\sum_{j \in C_1}(N_{ij}t_j - P_{ij}s_j) \quad (13)$$

is the total loss of this merger for the organization.

Proof:

Consider $C_1 \subseteq N, C_2 \subseteq N$, $C_1 \cap C_2 = \emptyset$, coalition value C_1 is:

$$v(S_1) = \sum_{i \in C_1}\sum_{j \in N} {P_{ij}}^T s_j - \sum_{i \in S_1}\sum_{j \in N} {N_{ij}}^T t_j - Cost(Q, C_1).$$

Using f and g defined above we have:

$$v(C_1) = \sum_{i \in C_1}\sum_{j \in C_1} P'_{ij}s_j + \sum_{i \in C_1}\sum_{j \in N \setminus C_1} P_{ij}s_j - \sum_{i \in C_1}\sum_{j \in C_1} N'_{ij}t_j - \sum_{i \in C_1}\sum_{j \in N \setminus C_1} N_{ij}t_j - Cost(Q, C_1)$$

Also have for coalition C_2:

$$v(C_2) = \sum_{i\in C_2}\sum_{j\in N}\bar{P}_{ij}{}^{T} s_j - \sum_{i\in C_2}\sum_{j\in N}\bar{N}_{ij}{}^{T} t_j - Cost(Q, C_2) = \sum_{i\in C_2}\sum_{j\in C_2} P'_{ij}s_j + \sum_{i\in C_2}\sum_{j\in N\setminus C_2} P_{ij}s_j - \sum_{i\in C_2}\sum_{j\in S_2} N'_{ij}t_j - \sum_{i\in C_2}\sum_{j\in N\setminus C_2} N_{ij}t_j - Cost(Q, C_2)$$

and for coalition $C_1 \cup C_2$:

$$v(C_1 \cup C_2) = \sum_{i\in C_1\cup C_2}\sum_{j\in C_1\cup C_2} P'_{ij}s_j + \sum_{i\in C_1\cup C_2}\sum_{j\in N\setminus C_1\cup C_2} P_{ij}s_j - \sum_{i\in C_1\cup C_2}\sum_{j\in C_1\cup C_2} N'_{ij}t_j - \sum_{i\in C_1\cup C_2}\sum_{j\in N\setminus C_1\cup C_2} N_{ij}t_j - Cost(Q, C_1 \cup C_2)$$

Replacing the equations relating $v(C_1 \cup C_2) \leq v(C_1) + v(C_2)$. Necessary and sufficient condition for the theory comes from.

Theory 2: consider non-ideal working environment, Coalition $C_1 \cup C_2$ Should not be created if and only if

$$\alpha \geq \frac{\lambda}{D(C_1 \cup C_2)} \tag{14}$$

Where

$$D(C_1 \cup C_2) := \sum_{i\in C_1}\sum_{j\in C_2}(F_{ij} + F_{ji}) \tag{15}$$

is general differences between members C_1, C_2.

Proof: Cost function for $C_1 \cup C_2$:

$$Cost(D, C) = \begin{cases} \alpha.\sum_{i\in C}\sum_{j\in C} D_{ij} + \beta|C| & if\ |C| > 1 \\ 0 & otherwise \end{cases}$$

with this definition:

$$Cost(D, C_1 \cup C_2) = \alpha.\sum_{i\in C_1\cup C_2}\sum_{j\in C_1\cup C_2} D_{ij} + \beta|C_1 \cup C_2|$$

$$\Rightarrow Cost(D, C_1 \cup C_2) = \alpha.\sum_{i\in C_1}\sum_{j\in C_1} D_{ij} + \alpha.\sum_{i\in C_2}\sum_{j\in C_2} D_{ij} + \alpha.\sum_{i\in C_1}\sum_{j\in C_2}(D_{ij} + D_{ji}) + \beta|C_1| + \beta|C_2|$$

$$\Rightarrow Cost(D, C_1 \cup C_2) = Cost(D, C_1) + Cost(D, C_2) + \alpha\,\text{Total}(C_1 \cup C_2).$$

This theory show lower bound on the cost per unit where cooperation for two coalition losses, in fact show these divisions are incompatible. This means that when forming coalitions the lowest α among α with positive values are chosen, because that α show coalitions that less distance to bring the organization to less utility and the role of these incompatible sectors are more bold.

3. Validation

It is always interesting to validate the results of the implementation of our proposed model on the real-world case study of this paper.

a) About the Case Study Organization

The center has three important information parts:

1. Education
2. Finance Section
3. Technology Department

Education in fact is considered very important and Main and all the information needed both financial and IT sector provides. The financial sector using of information of education sector is calculated student semester fees and the IT sector using Information taken from the education sector put courses for student in related page for student.

The first pre-processing of the necessary research been done and then do a little building was desired. To reach this goal the preparation of questionnaires, each of the managers based on their experiences of their comments were announced.

For the given case study, the set of all players is the set of all divisions, i.e., $n = \{1, 2, 3\}$.

These three sector have vectors security sources $s: = [10, 5, 7]$, and, Vector threats against vulnerabilities $t: = [18, 3, 5]$

Matrices of positive and negative impact on another sector organization using a questionnaire were obtained as follows:

$$P = \begin{bmatrix} 1 & 0.7 & 0.8 \\ 0.6 & 1 & 0.1 \\ 1 & 0.1 & 1 \end{bmatrix} \tag{16}$$

$$\mathrm{N} = \begin{bmatrix} 1 & 0.5 & 0.9 \\ 0.2 & 1 & 0 \\ 0.5 & 0 & 1 \end{bmatrix} \tag{17}$$

To initialize in the differences matrix, we use Licert's 5-degree spectrum and if between sections was not the different, puts Zero.

Very high	High	Average	Low	Very low
2.5	2	1.5	1	0.5

Table 2. Likert's 5-degree spectrum

So the difference matrix is calculated as follows:

$$D = \begin{bmatrix} 0 & 0.5 & 1 \\ 2.5 & 0 & 0 \\ 2.5 & 0.5 & 0 \end{bmatrix} \quad (18)$$

Considering we have $\beta = 1$, try with data obtained to specify incompatible divisions that minimizes the total utility of organization as the price per unit friction α varies.

Coalition 1 and 2:

$$\lambda = (0.5 * 18 - 0.7 * 10) + (0.2 * 3 - 0.6 * 5) = -0.4$$

$$\alpha \geq \frac{\lambda}{Total(C_1 \cup C_2)} = -0.13$$

Coalition 1 and 3:

$$\lambda = (0.9 * 18 - 0.8 * 10) + (0.5 * 5 - 1 * 7) = 3.7$$

$$\alpha \geq 1.05$$

Coalition 2 and 3:

$$\lambda = (-0.1 * 5) + (-0.1 * 7) = -1.2$$

$$\alpha \geq -2.4$$

Considering that the amount of α cannot be negative, so the coalition that should be discussed , first and third.

Initial utility for organization is each value, utility formed this coalition is equal to -34. Then total utility organization formed from incompatible divisions becomes less.

4. Limitation

Since Information security and also Risk Management are still areas which need to improve in some Iranian universities, we couldn't consider them in our analysis. On the other hand, due to questionnaire limitation, the study's sample size is 1. This size may be considered large for our statistical analysis.

5. Conclusion

In this research we prepare a questionnaire to evaluate Incompatible parts and also risk management in University of Science and Technology E-Learning Center and studying the Incompatible parts impacts on utility of organization. In general, by collecting data and analyzing them, the survey showed that Incompatible parts of organizations have negative impacts on utility of organization risk management process. Furthermore, it adds values to other organizations and provides the best practices in planning, developing, implementing and monitoring risk management in organizations.

References

Alberts, C.J., & Dorofee, A.J. (2001). OCTAVE criteria version 2.0. CMU/SEI- 2001-TR-016. ESC-TR-2001-016.

Alpcan, T., & Basar, T. (2004). A game theoretic analysis of intrusion detection in access control systems. *Proceedings of the 43rd IEEE Conference on Decision and Control (CDC).* IEEE, 2, 1568-1573. https://doi.org/10.1109/cdc.2004.1430267

Arshad, N.H., Mohamed, A., & Mansor, R. (2009). The Effects of Implementing Organizational Structural and Risk Management Strategies in Information System Projects. *Proceedings of the 10th WSEAS Int. Conference on Mathematics and Computers in Business and Economics.*

Chai, S., Kim, M., & Raghav-Rao, H. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems,* 50, 651-661. https://doi.org/10.1016/j.dss.2010.08.017

Chatzoglou, P.D., & Diamantidis, A.D. (2009). IT/IS implementation risks and their impact on firm performance. *International Journal of Information Management,* 29, 119-128. https://doi.org/10.1016/j.ijinfomgt.2008.04.008

Colwill, C. (2009). Human factors in information security: The insider threat e Who can you trust these days? *Information Security Technical Report, 14(4)*, 186-196. https://doi.org/10.1016/j.istr.2010.04.004

Dlamini, M.T., Eloff, J.H.P., & Eloff, M.M. (2009). Information security: The moving target. *Computers & Security,* 28, 189-198. https://doi.org/10.1016/j.cose.2008.11.007

Golany, B., Kaplan, E.H., Marmur, A., & Rothblum, U.G. (2009). Nature plays with dice terrorists do not allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research,* 192(1). https://doi.org/10.1016/j.ejor.2007.09.001

Gordon, L.A., Loeb, M.P., & Tseng, C.Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *J. Account. Public Policy*, 28, 301-327. https://doi.org/10.1016/j.jaccpubpol.2009.06.006

Hausken, K., & Levitin, G. (2009). Mini max defens strategy for complex multi-state systems. *Reliability Engineering and System Safety,* 94. https://doi.org/10.1016/j.jaccpubpol.2009.06.006

Hogganvik, I. (2007). *A graphical approach to security risk analysis.* Oslo, Norway: University of Oslo, Faculty of Mathematics and Natural Sciences.

Howard, M., & LeBlanc, D. (2002). *Writing secure code.* Redmond, WA, USA: Microsoft Press.

Kantzavelou, I., & Katsikas, S. (2009). Playing Games with Internal Attackers Repeatedly. *Proceedings of the 16th IEEE Conference on Systems, Signals and Image*. https://doi.org/10.1109/iwssip.2009.5367708

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers and Security,* 24, 147-59. https://doi.org/10.1016/j.cose.2004.07.004

Lima, D.A., Contreras, J., & Feltrin, A. (2008). A cooperative game theory analysis for transmission loss allocation. *Electric Power Systems Research,* 78, 264-275. https://doi.org/10.1016/j.epsr.2007.02.008

Liu, D., Wang, X., & Camp, J. (2008). Game-theoretic modeling and analysis of insider threats. *International Journal of Critical Infrastructure Protection,* 1. https://doi.org/10.1016/j.ijcip.2008.08.001

Liu, P., & Zang, W. (2005). Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Trans. Inf Syst Secur,* 8(1), 78-118. https://doi.org/10.1145/1053283.1053288

Miura-Ko, R.A., Yolken, B., Mitchell, J., & Bambos, N. (2008). Security decision-making among interdependent organizations. *Stanford University, Computer Security Foundations Symposium, IEEE.* https://doi.org/10.1109/csf.2008.25

Morris, P. (1994). *Introduction to Game Theory* (First Ed.). Springer. https://doi.org/10.1007/978-1-4612-4316-8

Myerson, R.B. (1991). *Game Theory, Analysis of Conflict*. Cambridge, MA, USA: Harvard University Press.

Saad, W., Alpcan, T., Basar, T., & Hjørungnes, A. (2010). Coalitional Game Theory for Security Risk Management. *The Fifth International Conference on Internet Monitoring and Protection (ICIMP)*. Barcelona, Spain. https://doi.org/10.1109/ICIMP.2010.14

Schechter, S.E. (2004). *Computer security strength & risk: a quantitative approach*. PhD Thesis. Boston, USA: Harvard University.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security. Journal,* 16, 315-331.

Yildirim, E.Y., Akalp, G., Aytac, S., & Bayram, N. (2010). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*.