Agris on-line Papers in Economics and Informatics

Volume VIII Number 1, 2016

Information Security Management: ANP Based Approach for Risk Analysis and Decision Making

H. Brožová[1], L. Šup[2], J. Rydval[1], M. Sadok[3], P. Bednar[4]

[1] Faculty of Economics and Management, Czech University of Life Sciences Prague, Czech Republic

[2] Faculty of Economics and Management and Dept. of Security, Czech University of Life Sciences Prague, Czech Republic

[3] Higher Institute of Technological Studies in Communication in Tunis, Tunisia and School of Computing, University of Portsmouth, UK

[4] School of Computing, University of Portsmouth, UK, and Dept. of Informatics, Lund University, Sweden

Abstract

In information systems security, the objectives of risk analysis process are to help to identify new threats and vulnerabilities, to estimate their business impact and to provide a dynamic set of tools to control the security level of the information system. The identification of risk factors as well as the estimation of their business impact require tools for assessment of risk with multi-value scales according to different stakeholders' point of view. Therefore, the purpose of this paper is to model risk analysis decision making problem using semantic network to develop the decision network and the Analytical Network Process (ANP) that allows solving complex problems taking into consideration quantitative and qualitative data. As a decision support technique ANP also measures the dependency among risk factors related to the elicitation of individual judgement. An empirical study involving the Forestry Company is used to illustrate the relevance of ANP.

Keywords

Information security, Risk factors, Semantic networks, Analytical network process, Multi-criteria decision making, Case Study.

Brožová, H., Šup, L, Rydval, J., Sadok, M. and Bednar, P. (2016) "Information Security Management: ANP Based Approach for Risk Analysis and Decision Making", *AGRIS on-line Papers in Economics and Informatics*, Vol. 8, No. 1, pp. 13 - 23. ISSN 1804-1930. DOI: 10.7160/aol.2016.080102.

Introduction

The pervasive uses of and dependencies on information technologies have increased security risks which can induce losses in companies revenue and reputation. Despite the external sources of security attacks, internal abuse and malicious activity may generate an unexpected damage. Companies protect their networks by means of ad hoc security solutions such as access control measures, procedures to prevent and respond to security incidents and risk assessment. The review of the common risk analysis frameworks reveals four mainly steps. They are (a) the classification of information assets according to their sensitivity, (b) the identification of the threats and vulnerabilities, (c) the likelihood occurrences and impact estimation of these threats and (d) the implementation of controls and corrective countermeasures taking into consideration their cost.

In this paper we explore the potential relevance of the Analytical Network Process (ANP) use in information systems security (ISS) context to support the development of individual understanding of security risks leading to richer elaboration of problem spaces. The identification of a number of risk factors requires a classification according to their severity and impact on the information system activity. However, this classification should pay attention to the influence of contextual variables such as the exploration of multiple perspectives of contextual understanding of security risk factors. The involvement of organizational stakeholders to assess security risks with multi-value scales would result in a better understanding of the role

and application of security functions in situated practices and an achievement of contextually relevant risk analysis (Bednar and Katos, 2010, Sadok et al., 2014).

In fact, a number of researchers have identified qualitative and quantitative approaches of IS risk analysis. The reliability of qualitative methods is based on the subjective assessments of experts during the evaluation process (Klimeš and Bartoš, 2015, Bartoš and Walek, 2013, Walek et al., 2013). The quantitative methods are mainly based on mathematical models and can be divided into: i) deterministic methods, ii) probabilistic methods, iii) methods using analogies, and iv) multi-criteria evaluation methods (EIC/ISO). As to the multi-criteria evaluation methods, Delphi method is often used to evaluate risk factors (Briš, 2009, Procházková, 2011b). However and in order to overcome the drawbacks of available risk analysis approaches, Klimeš and Bartoš (2015) suggested fuzzy approach to decision making process based on six sub processes and including several IF-THEN-rule knowledge bases.

Although ANP as a decision support technique has the potential to measure the dependency among security risk factors it is not commonly used in the Czech Republic (Procházková, 2011a). Few studies have been applied ANP to assess the importance of individual elements of the consumer's behaviour of the framing effect (Rydval, 2011, Rydval and Bartoška, 2013, Rydval and Brožová, 2011). As to the Delphi method the ANP uses experts' judgement. It is noticeable that more experts are involved in the evaluation process more relevant the final assessment is.

Consequently, our approach is firstly based on the identification of crucial and significant risk factors leading to the threats and vulnerabilities of information systems. Secondly, the risk factors and relationships between them are described using semantic network in order to develop the decision network. The ANP is then used for the priority evaluation of these factors (Brožová et al., 2015). This leads to a better definition and implementation of effective security countermeasures.

The remainder of this paper is organized as follows. In section 2, a short review of ANP and semantic network concepts found in literature are provided. In section 3 scenarios of security risk factors are described. The section 4 presents the results of an empirical study conducted in the forestry company. Finally, concluding remarks are presented in section 5.

Materials and methods

Semantic network

Semantic network illustrates different points of view as well as the relationships between different relevant elements within a decision context. In effect, semantic networks were originally used to express meanings of various expressions in natural language. According to Sowa (2000) semantic networks are used namely because of their ability to easily provide usable system to represent information and to mainly focus on the organization of a large number of information sources. They also support the description of complex processes and offer a tool to represent the understanding of a problem space.

Semantic (associative) network is defined as a directed graph consisting of nodes and edges (Sowa, 2000). Nodes represent items of described problem and edges connecting these nodes represent relationships between these items. Fundamental types of these relations are as follows:

- IS-AN-INSTANCE-OF (IIO) relationship is used to state that a particular object (instance of a particular class) belongs to the specified class.
- IS-A-KIND-OF (IKO) relationship is used to state that a class is a subclass of another class.
- IS-A-PART-OF (IPO) relationship is used to state that a certain class of objects is composed of some parts.

The semantic network of the decision problem can be used as a starting point for the creation of the ANP decision network. The basic advantage of the semantic network is that it contains information similar to information stored in the human memory, and it is machine-understandable. This means that it can be machine-processed. Therefore, it is possible to analyse facts and information included in the semantic network and to acquire new knowledge about represented facts (Steyvers and Tenenbaum, 2005, Xia and Bu, 2012).

ANP method

The ANP is a multiple criteria decision method based on the network representation of a decision problem which considers the dependence across elements and levels of a decision problem (Saaty, 2001, 2003). The crucial step of the ANP is the pairwise comparison of all pairs of elements related to the same element from higher level

or different cluster from decision network. The steps of the ANP method for this study are as follows:

1. The first step – the semantic network describing the elements of the ISS decision problem and their relationships are constructed.
2. The second step - the network is created based on the semantic network to describe inner dependence within a set (clusters) of decision elements, and outer dependence among different sets (clusters) of the decision elements.
3. The third step - the pairwise comparisons of the elements within and across the clusters are made. The consistency of these comparisons is also checked.
4. The fourth step - if the comparison is not consistent, the decision maker will see how to change and adjust the comparison (Hlavatý, 2014).
5. The fifth step - the normalized supermatrix with the preferences derived from the previous pairwise comparisons is calculated.
6. The sixth step - the limiting supermatrix is computed using program SuperDecision and global preferences of decision elements are obtained (Saaty, 2001).

Evaluation of the pairwise comparisons

The importance of each factor is made using Saaty pairwise comparison of all factors related to the factor or cluster on the higher level (Saaty, 2008). The pairwise comparison is used to estimate the importance of ISS factors in pairs from different points of view. A single number from the fundamental 1–9 scale are standardly used for expert estimation. The Table 1 shows the explanation of each value in this scale in the ISS context comparison of the first and second factor from the pair.

This evaluation could be made for example by a security expert. His judgement has to be consistent, if not we use simple role showing how to improve judgement consistency. The range of feasible values of each preference in Saaty's matrix can be computed from assuming the inconsistency index must not reach over the threshold and ideal values of the selected intensity relatively to the other values on the basis of requirement that the consistency index is equal to 0 (Hlavatý, 2014). If the values in Saaty's matrix are not consistent, ideal values are calculated and the expert got a feedback and an advice on how to adjust the comparison. After this process we obtain the consistent Saaty matrices and the ANP model is calculated by SuperDecision software.

Calculation of the limit matrix

The calculation of the synthetized weights (for example preferences of ISS factors) is then provided using the software SuperDecisions (SuperDecision). The synthetized weights are calculated in the limit matrix. The input to the limit matrix calculation is the normalized supermatrix, which is a matrix of local weights, i.e. preferences derived from the previous pairwise comparisons. The standard steps of the limit matrix calculation are (Saaty, 2001).

1. Raise the matrix to larger powers, and either,
2. The powers will converge to the limit matrix, or
3. The powers will converge to a cycle of matrices and the limit matrix is the average of these.

This algorithm performs remarkably well except in two circumstances (Adams, 2011):

- Hierarchies: In the case of hierarchies the large powers of normalized supermatrix

Intensity of importance	Definition	Explanation
1	Equal Importance	Two factors equally important for ISS
3	Moderate importance	Experience and judgment slightly favour the first ISS factor over the second one
5	Strong importance	Experience and judgment strongly favour the first ISS factor over the second one
7	Very strong or demonstrated importance	The first ISS factor is favoured very strongly over the second one; its importance demonstrated in practice
9	Extreme importance	The highest possible degree of preference of the first ISS factor over the second one

Source: own processing according to Saaty (2008)

Table 1: Fundamental scale of pairwise comparison of ISS factors.

eventually go to zero and then the limit matrix contains all zeros (in other words no nodes get any scores of preferences).

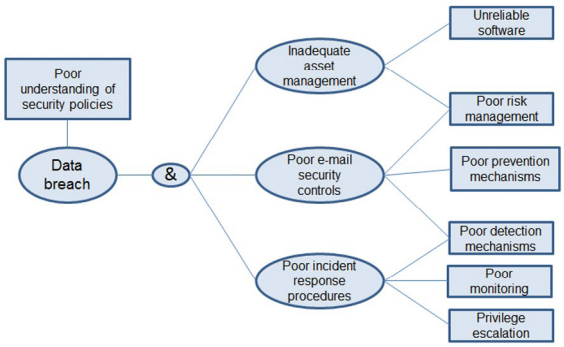
- Sinks in general: Even in networks with feedback, if there are sinks in the network (nodes without connections emanating from them) then the large powers of the normalized supermatrix will still tend toward zero (at least many columns of the limit matrix tend to zero).

Identity at sinks method is the standard approach to avoid this problem with calculation the limit matrix for hierarchies as well as networks with sinks adding self-loop to the sinks (Adams, 2011) and this does give correctly synthesized values for the sinks, but all other nodes get zeros from this calculation. This synthesis is used to determine the weights only of ISS factors which lies in the end nodes of the semantic network. These factors are considered primary in ensuring the ISS. Calculus Type method is another approach (similar philosophy as the differential calculus). This type of calculation again calculates large powers of the supermatrix, but these powers are normalized (Adams, 2011). This normalized supermatrix will not still tend toward zero and returns correctly synthesized values for all nodes in the network. This way we get the weights of all the elements of the semantic network.

Scenarios of security risk factors

In the particular context of ISS it is necessary to construct different scenarios of security risk factors reflecting different points of view. The comparison and integration of security risk factors within a semantic network provide an overview of the relative importance and impact of a particular security risk factor. This leads to identify the most important security risk factors and to assess their impact on the efficiency and effectiveness of an information system. Consequently, appropriate mitigation decisions to cope with and reduce security risks could efficiently be made.

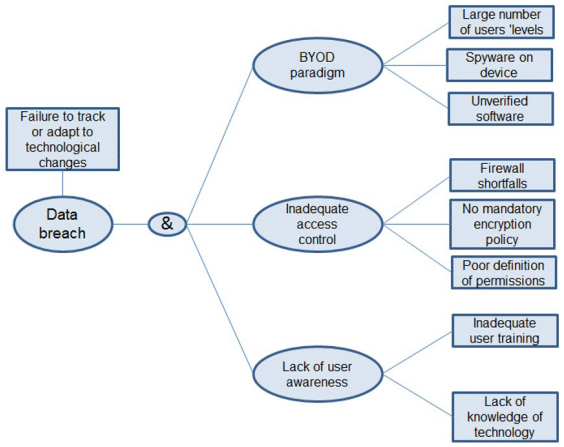
In this section we describe three diagrams as produced by three stakeholders (end user, network administrator, security expert) respectively following a security 'Data breach'. These diagrams contain the most relevant security risk factors and their relations. The view of the security expert related to possible security risk factors explaining the 'Data breach' is captured in Figure 1.



Source: Sadok et al., 2014

Figure 1: Security expert' diagram.

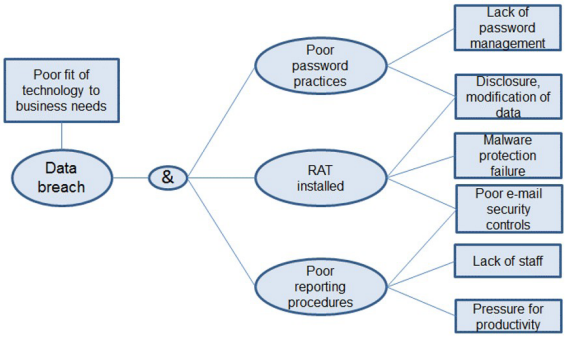
The view of the network administrator about possible security risk factors explaining the 'Data breach' is captured in Figure 2.



Source: Sadok et al., 2014

Figure 2: Network administrator' diagram.

The end user's view about possible security risk factors explaining the 'Data breach' is captured in Figure 3.



Source: Sadok et al., 2014

Figure 3: End user' diagram.

Semantic network as a tool for system analysis of the decision process is used for the description of the IS risk factors and its relations. It shows

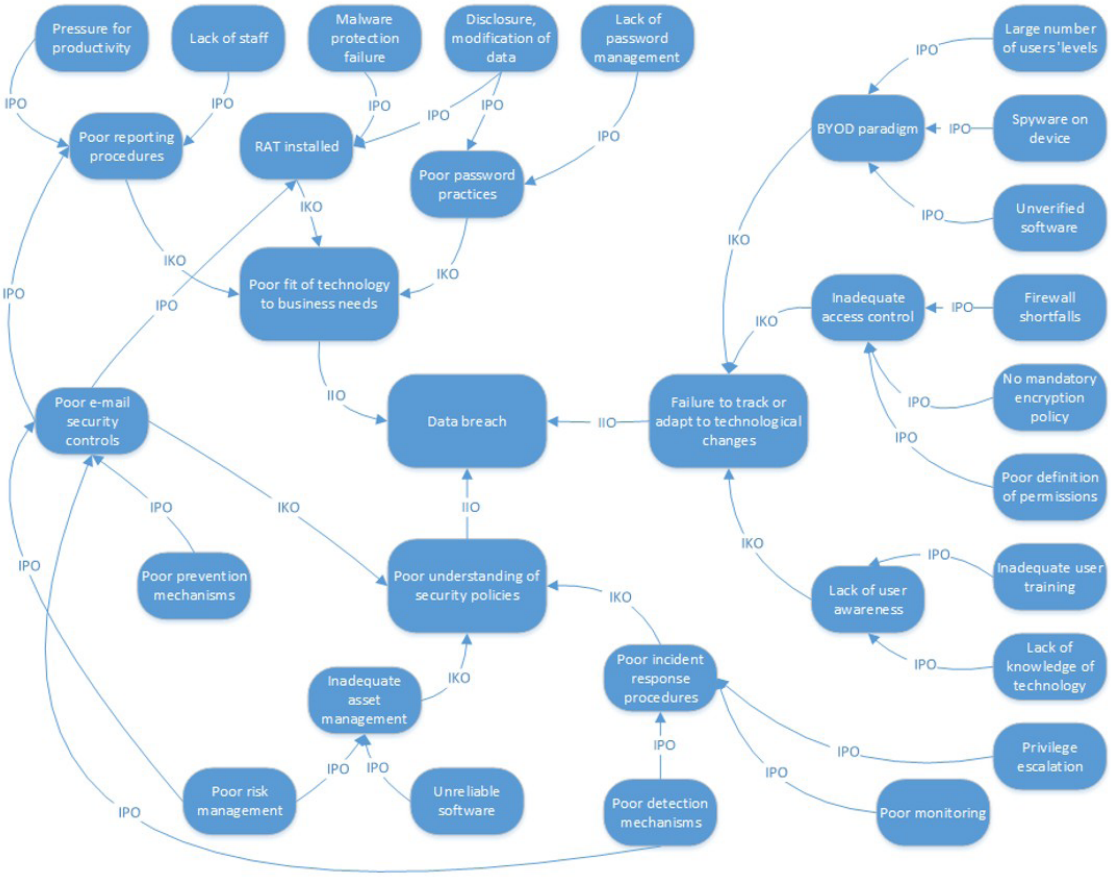
the structure of possible ISS factors, factors hierarchy, relations and factors influenced by different user groups. It can show individual elements influencing issues of 'Data breach'. It provides us with information about relationships in the network between individual factors of the ISS and how they can influence the threatened data. However, it does not give us the quantitative information about the importance of these factors and how much they influence the 'Data breach'. The semantic network is used as a decision network for the ANP method and the SuperDecision program (SuperDecision).

The Figure 4 shows that the issue of 'Data breach' consists of three main instances. They are: 'Poor understanding of security policies', 'Failure to track or adapt to technological changes', and 'Poor fit of technology to business needs'.

Each of these three major instances of the 'Data breach' incorporates various elements expressing different possibilities of the instances development. These elements could be divided into a different number of sub elements describing the component parts of the element responsible for a particular instance of the 'Data breach'.

Some elements, respectively sub-elements can play multiple roles within the semantic network because of the differences between the three points of view. The role of the element and its affiliation to the class of elements or sub-elements is displayed in the Figure 4 using evaluated connection between the elements (IIO, IKO or IPO). For example, the element 'Poor e-mail security controls' plays two kinds of roles. First it is a kind of instance of item 'Poor understanding of security policies' (oriented connection IKO) and second it is a part (sub-element) of the element 'RAT installed' (connection IPO).

The pairwise comparison of items of the created decision network is then made by different groups in the organisation including managers, security experts and end users. This judgement is initially filled in special form in MS Excel (Table 2) which helps users to make consistent decisions during the comparison process.



Source: own processing

Figure 4: Semantic Network of 'Data breach'.

A - most important	Equally									B - most important
A	9	7	5	3	1	3	5	7	9	B
Poor password practices	x									Poor reporting procedures
Poor password practices						x				RAT installed
Poor reporting procedures								x		RAT installed

Source: own processing

Table 2: MS Excel form for pairwise comparisons.

				Weights						
Poor reporting procedures	1.000	9.000	0.333	**0.324**	*-2.206*	*9.000*	*0.333*	*Lambda*	*3.2056*	**Consistency index**
RAT installed	0.111	1.000	0.143	**0.056**	*0.111*	*-2.206*	*0.143*	*Determinant*	*-6E-05*	**0.10**
RAT installed	3.000	7.000	1.000	**0.62**	*3.000*	*7.000*	*-2.206*			
		Ideal values		1						
		1.167	**0.643**							
			0.019							

Source: own processing

Table 3: Ideal values for pairwise comparisons.

After the user files this table the consistency index is computed. If the comparisons are not consistent the automatic calculation shows ideal value of each individual preference relatively to the others two values. These ideal values can support the adjustment of the initial evaluation in case it is not consistent (Table 3).

Results and discussion

The forestry company

Although the dependency of agricultural and forestry companies on IT use is not very high it is not anymore conceivable for these companies to miss the benefits of such use. In fact, the sustainability and competitiveness of their activities are intimately based on the effectiveness and efficiency of their information systems management. However, it is necessary to secure information systems assets to ensure business continuity and economic profits.

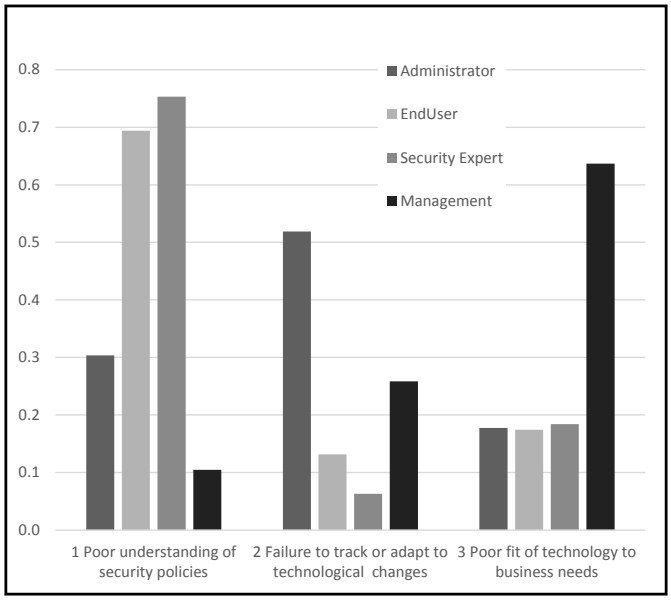
In this section, we describe the application of ANP for risk management in a particular agricultural enterprise. *Vojenské lesy a statky ČR*, a state enterprise, is an organization with a history that goes back to more than eighty years. *Vojenské lesy a statky ČR* manage an area of more than 126,000 hectares of forest land and more than 6,000 hectares of agricultural land and water area. It is one of the largest organizations of its type in the Czech Republic. Its main activities include forest management, trade in timber, hunting, fishing, agricultural activity, nature protection among others. The objective of the enterprise is, in line with the assignment from its founder, the Ministry of Defence of the Czech Republic, to be at the top in the field of forest-based industry and agricultural production. It aims to maintain sustainable forest and agricultural ecosystems using modern technology and knowledge with respect to the environment and maintaining natural landscape features. There is a separate ICT department within *Vojenské lesy a statky* which is in charge of supporting information systems activities and users. In enterprises of such size (more than 2,000 employees), an important number of supporting information systems are used, and the organization information assets are very valuable. As a result, the failure or any actions that compromises the availability, confidentiality or integrity of these assets would cause significant negative impact on the enterprise's operations and performance.

Expert evaluation of the ANP model according to the proposed structure was obtained during discussions with end users, IS network administrators, security experts and also one manager from the same company. Their judgments were checked for their consistency and slightly modified if necessary according to the ideal values guideline. End users evaluated the ISS factors from the group 'Poor fit of technology to business needs', security expert compared factors from the group 'Poor understanding of security policies' and network administrator from the group 'Failure to track or adapt to technological changes'. Manager and all users compared also these three groups. The Table 4 and Figure 5 show weights

Groups of ISS factors	Administrator	End User	Security Expert	Management
1 Poor understanding of security policies	0.303510	0.694061	0.753111	0.104725
2 Failure to track or adapt to technological changes	0.518996	0.131510	0.062917	0.258292
3 Poor fit of technology to business needs	0.177494	0.174429	0.183972	0.636982

Source: own processing

Table 4. Weights of groups of ISS factors.



Source: own processing

Figure 5: Weights of groups of ISS factors.

of three groups of ISS factors. Factors included in 'Poor understanding of security policies' are seen very important for all except for management (all individual weights are greater than 0.3). Generally managers feel 'Poor fit of technology to business needs' as higher important (more than 0.6). Network administrator gives higher importance to ISS factors 'Failure to track or adapt to technological changes' (more than 0.5).

Global importance or synthesized preferences of the partial ISS factors are calculated in the limit matrices. Limit matrix received by Calculus type method (Table 5, Figure 6) shows most important ISS factors from all (preferences higher than 0.07). These factors are mainly from the first ISS factors group ('Poor understanding of security policies') according to the network administrator, end users and security expert. Management also gives the high priority to the factors from the third group of the ISS factors ('Poor fit of technology to business needs').

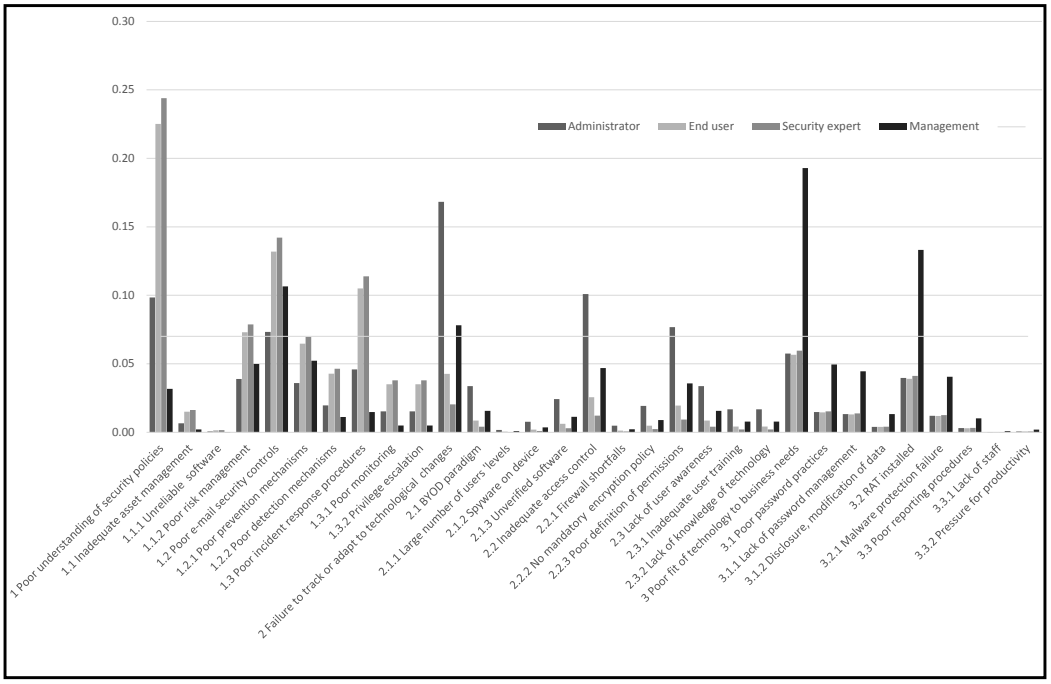
When the Identity of sink method is used, the highest preferences of primary ISS factors are calculated (Table 5, Figure 7). Eight ISS factors can be seen as important ISS factors from different points of view (preferences higher than 0.1). The first six factors 'Poor risk management', 'Poor prevention mechanisms', 'Poor detection mechanisms', 'Poor monitoring', 'Privilege escalation', and 'Poor definition of permissions' are evaluated as very important from practically all stakeholders. The last two factors 'Lack of password management', and 'Malware protection failure' are considered of high importance from the management point of view.

These results are coherent with and support previous works on ISS with a socio-technical perspective. In effect, rather than a dominant emphasis on technologies, for instance, it is essential to fund processes that fully bridge the gap between design and implementation of secure and usable systems through open discussion and dialogue between relevant stakeholders leading to better contextual appreciation of risks. It is also necessary to understand how organizational and environmental factors as well as compliance behavior may affect the efficient use of security controls and policies.

	Administrator		End User		Security Expert		Management	
	Identity sink	Calculus type	Identity sink	Calculus type	Identity sink	Calculus type	Identity sink	Calculus type
1 Poor understanding of security policies		0.0984		0.2251		0.2439		0.0317
1.1 Inadequate asset management		0.0066		0.0150		0.0163		0.0021
1.1.1 Unreliable software	0.0020	0.0007	0.0046	0.0015	0.0050	0.0016	0.0007	0.0002
1.1.2 Poor risk management	0.1201	0.0389	0.2250	0.0730	0.2430	0.0787	0.1582	0.0499
1.2 Poor e-mail security controls		0.0733		0.1320		0.1422		0.1065
1.2.1 Poor prevention mechanisms	0.1108	0.0359	0.1994	0.0647	0.2151	0.0697	0.1652	0.0522
1.2.2 Poor detection mechanisms	0.0606	0.0196	0.1321	0.0428	0.1431	0.0464	0.0362	0.0112
1.3 Poor incident response procedures		0.0459		0.1051		0.1138		0.0148
1.3.1 Poor monitoring	0.0472	0.0153	0.1080	0.0350	0.1172	0.0379	0.0163	0.0049
1.3.2 Privilege escalation	0.0472	0.0153	0.1080	0.0350	0.1172	0.0379	0.0163	0.0049
2 Failure to track or adapt to technological changes		0.1683		0.0427		0.0204		0.0782
2.1 BYOD paradigm		0.0337		0.0085		0.0041		0.0156
2.1.1 Large number of users 'levels	0.0053	0.0017	0.0013	0.0004	0.0006	0.0002	0.0026	0.0008
2.1.2 Spyware on device	0.0236	0.0076	0.0060	0.0019	0.0029	0.0009	0.0117	0.0036
2.1.3 Unverified software	0.0749	0.0243	0.0190	0.0062	0.0091	0.0029	0.0373	0.0113
2.2 Inadequate access control		0.1010		0.0256		0.0122		0.0469
2.2.1 Firewall shortfalls	0.0150	0.0049	0.0038	0.0012	0.0018	0.0006	0.0074	0.0023
2.2.2 No mandatory encryption policy	0.0595	0.0193	0.0151	0.0049	0.0072	0.0023	0.0296	0.0090
2.2.3 Poor definition of permissions	0.2369	0.0768	0.0600	0.0195	0.0287	0.0093	0.1179	0.0357
2.3 Lack of user awareness		0.0337		0.0085		0.0041		0.0156
2.3.1 Inadequate user training	0.0519	0.0168	0.0132	0.0043	0.0063	0.0020	0.0258	0.0078
2.3.2 Lack of knowledge of technology	0.0519	0.0168	0.0132	0.0043	0.0063	0.0020	0.0258	0.0078
3 Poor fit of technology to business needs		0.0575		0.0566		0.0596		0.1929
3.1 Poor password practices		0.0148		0.0145		0.0153		0.0495
3.1.1 Lack of password management	0.0410	0.0133	0.0403	0.0131	0.0425	0.0138	0.1472	0.0446
3.1.2 Disclosure, modification of data	0.0122	0.0040	0.0120	0.0039	0.0127	0.0041	0.0439	0.0133
3.2 RAT installed		0.0397		0.0391		0.0411		0.1331
3.2.1 Malware protection failure	0.0373	0.0121	0.0366	0.0119	0.0386	0.0125	0.1338	0.0405
3.3 Poor reporting procedures		0.0031		0.0030		0.0032		0.0102
3.3.1 Lack of staff	0.0008	0.0002	0.0007	0.0002	0.0008	0.0003	0.0146	0.0008
3.3.2 Pressure for productivity	0.0018	0.0006	0.0017	0.0006	0.0018	0.0006	0.0093	0.0019

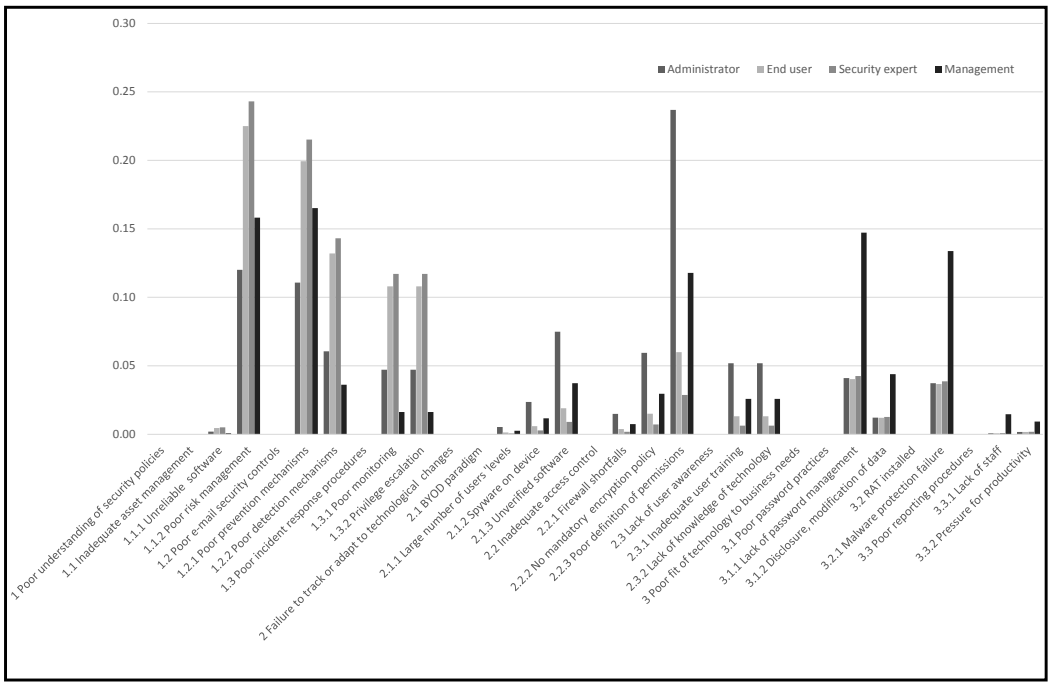
Source: own processing

Table 5: Weights of ISS factors.



Source: own processing

Figure 6: Weights of ISS factors by Calculus type method.



Source: own processing

Figure 7: Weights of ISS factors by Identity at Sinks method.

Conclusion

This paper aimed to shed light on the challenge of introducing security in a sensible and useful manner by addressing the contextual perspectives. The identification of security risk factors as well as the estimation of their business impact require tools for assessment of risk with multi-value scales according to different stakeholders' point of view. We argue in this paper that ANP provides a relevant approach to assess security risk factors taking into consideration quantitative and qualitative data. A case study is discussed to illustrate such relevance. The understanding of the importance

of security risk factors support the definition and implementation of efficient and effective security controls and policies.

Recognizing the complexity nature of security risk management, a number of implications for practitioners and researchers can be identified and should be deeply addressed. For example, to assist and facilitate assessment of risk with multi-value scales according to different stakeholders' point of view, a potential interdisciplinary research area emerges to develop techniques and modelling support for analysis aiming at inquiries into uncertain and complex problems spaces.

Acknowledgements

This research is supported by the Internal Grant Agency of the University of Life Sciences Prague – project IGA PEF 20151027 - The use of the Analytic Network Process to identify and to assess security risks of Information Technologies projects.

Corresponding author:
RNDr. doc. Helena Brožová, CSc.
Department of System Engineering, Faculty of Economics and Management
Czech University of Life Sciences Prague, Kamýcká 129, 165 21 Prague 6 - Suchdol, Czech Republic
E-mail: brozova@pef.czu.cz

References

[1] Adams, B. (2011) "SuperDecisions Limit Matrix Calculations". USA: Decision Lens Inc.

[2] Bartoš, J. and Walek, B. (2013) "A methodology for testing of information system under uncertainty." In: *Proc. 36th International Conference on Telecommunications and Signal Processing (TSP)*, Faculty of Electrical Engineering and Communication, Brno University of Technology, Brno, pp. 20-22.

[3] Bednar, P. and Katos, V. (2010) "*Digital forensic investigations: a new frontier for Informing Systems, in D'Atri, A. and Sacca, D."* (Ed.) Information Systems: People, Organizations, Institutions and Technologies, Springer Physica-Verlag, Berlin Heidelberg. ISBN 978-3-7908-2147-5.

[4] Briš, R. (2009) "*Reliability, Risk and Safety: Theory and Applications"*. CRC Press / Balkema, Leiden, 2009, ISBN 978-0-415-55509-8.

[5] Brožová, H., Šup, L., Rydval, J., Sadok, M. and Bednar, P. "Security risk factors: ANP model for risk management decision making." In: *Proceedings of the 33st International conference on Mathematical Methods in Economics*. University of West Bohemia, Cheb, pp. 74-79. ISBN 978-80-261-0539-8.

[6] Hlavatý, R. (2014) "Saaty`s matrix revisited: Securing the consistency of pairwise comparisons", In: *Proceedings of the 32st International conference on Mathematical Methods in Economics*. Palacký University, Olomouc, pp. 83–88. ISBN 978-80-244-4209-9.

[7] IEC/ISO (2009) "*Risk management – Risk assessment techniques IEC/ISO 31010"*. 1st ed. Geneva: ISO. ISBN 2-8318-1068-2.

[8] Klimeš, C. and Bartoš, J. (2015) "IT/IS Security Management with Uncertain Information", *Kybernetika*, Vol. 51, pp. 408-419, DOI: 10.14736/kyb-2015-3-0408.

[9] Procházková, D. (2011) "*Analýza a řízení rizik"*. Czech Technical University in Prague, Prague. ISBN 978-80-01-04841-2.

[10] Procházková, D. (2011) "*Metody, nástroje a techniky pro rizikové inženýrství"*. Karolinum, Prague. ISBN 978-80-01-04842-9.

[11] Rydval, J. and Bartoška, J. (2013) "*Quantification of Framing Effect in the Meat Distribution by ANP, Mathematical Methods in Economics"*, College of Polytechnics Jihlava. ISBN 978-80-87035-76-4.

[12] Rydval, J. and Brožová, H. (2011) "Quantification of Framing effect in education Process using ANP". In: *Proceedings of Efficiency and Responsibility in Education International Conference 2011*, Prague, CULS. ISBN 978-80-213-2183-0.

[13] Rydval, J. (2011) "Quantification of Framing Effect using ANP and AHP". I*n Mathematical Methods in Economics 2011*, Janska Dolina, Slovakia, Professional Publishing. ISBN 978-80-7431-058-4.

[14] Saaty, T. L. (2001) "*Decision Making with Dependence and Feedback: The Analytic Network Process, The Analytic Hierarchy Process Series"*. Pittsburgh, Vol. IX, RWS Publications.

[15] Saaty, T. L. (2003) "*The Analytic Hierarchy Process (AHP) for Decision Making and the Analytic Network Process (ANP) for Decision Making with Dependence and Feedback"*. Creative Decisions Foundation.

[16] Saaty, T. L. (2008) "Relative Measurement and Its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors: The Analytic Hierarchy/Network Process", *Rev. R. Acad. Cien. Serie A. Mat.,* Vol. 102, No. 2, pp. 251–318.

[17] Sadok, M., Katos, V. and Bednar, P. (2014) "*Developing contextual understanding of information security risks"*, International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), Plymouth University.

[18] Sowa, J. F. (2000) "*Knowledge Representation: Logical, Philosophical, and Computational Foundations"*, Brooks/Cole Publishing Co., Pacific Grove, CA. ISBN-13: 978-0534949655.

[19] Steyvers, M. and Tenenbaum, J. B. (2005) "The Large-Scale Structure of Semantic Networks: Statistical Analyses and a Model of Semantic Growth", *Cognitive Science*, Vol. 29, pp. 41–78. ISSN 1551-6709, DOI: 10.1207/s15516709cog2901_3.

[20] SuperDecisions: Software for Decision-Making. [Online] Available: http://www.superdecisions.com/ [Accessed 25 October 2015].

[21] Walek, B., Bartoš, J. and Žáček, J. (2013) "*Proposal of The Expert System for Conducting Information Security Risk Analysis"*, *Proceedings of the International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing*. The Society of Digital Information and Wireless Communications, pp. 58-68.

[22] Xia, Z. Y. and Bu, Z. (2012) "Community detection based on a semantic network," *Knowledge-Based Systems*, Vol. 26, pp. 30-39. ISSN 0950-7051.