COMPUTERS & SECURITY 55 (2015) 100–112

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

The information systems' security level assessment model based on an ontology and evidential reasoning approach

Kresimir Solic [a,c,*], *Hrvoje Ocevcic* [b,c], *Marin Golub* [d]

[a] *Faculty of Medicine, University of Osijek, Josipa Huttlera 4, HR-31000 Osijek, Croatia*
[b] *Hypo–Alpe-Adria-Bank d.d., Slavonska avenija 6, 10000 Zagreb, Croatia*
[c] *Faculty of Electrical Engineering, University of Osijek, Josipa Huttlera 4, HR-31000 Osijek, Croatia*
[d] *Faculty of Electrical Engineering and Computing, Zagreb University, Unska 3, HR-10000 Zagreb, Croatia*

ARTICLE INFO

Article history:
Received 12 December 2014
Received in revised form 26 June 2015
Accepted 31 August 2015
Available online 5 September 2015

Keywords:
Information security model
Information security
Risk assessment
Security control selection
Security management
OWL
Ontology
Evidential reasoning

ABSTRACT

In the area of information technology an amount of security issues persists through time. Ongoing activities on security solutions aim to integrate existing security guidelines, best practices, security standards and existing solutions, but they often lack a knowledge base or do not involve all security issues, particularly human influence.

In this paper, we presented a model that can be the basis for a novel information systems security evaluation solution. This solution should be able to cover a wide range of all possible information security issues. Our model is based on an OWL ontology for knowledge base, uses an enhanced Evidential Reasoning algorithm for mathematical calculations and possesses a simple reflex intelligent agent's algorithm as a decision supporting element.

Properties for this model supervene from properties of its constructing elements. Knowledge base being built on OWL ontology is a major element of the model. It can provide high flexibility and applicability to different information systems and business organizations; upgradeability to be up to date regarding current security issues and new threats; and high versatility, taking into evaluation all possible aspects regarding security issues, e.g., network security, software and hardware issues, human influence, security policies and disaster recovery plans. Enhanced Evidential Reasoning algorithm is based on the Dumpster–Shafer theory and is well suited for calculations with expert's subjective judgements combining qualitative with quantitative evaluation grades. We designed an algorithm for back coupling based on a simple reflex intelligent agent for results presentation and decision support.

In our work, we explained how to connect and use each of the model's constructive elements to obtain information security evaluation results. In addition, we conducted a case study with the proposed model on a small business organization. To test our model, we also used the standard qualitative risk assessment method on the same business organization in order to compare both qualitative results.

Preliminary testing results have shown that the presented model could achieve its goal if it would be developed into an integrated software tool with a well-defined and up-to-date ontological knowledge base.

* *Corresponding author.* Tel.: +385 917550631.
E-mail addresses: kresimir.solic@mefos.hr (K. Solic), hrvoje.ocevcic@hypo-alpe-adria.hr (H. Ocevcic), marin.golub@fer.hr (M. Golub).
http://dx.doi.org/10.1016/j.cose.2015.08.004
0167-4048/

1. Introduction

An amount of information security problem issues persist through time, even though there are different security guidelines and software tools for security evaluation and risk management that cover different approaches and solve different security issues. Additionally, business managers and security experts often use different terms for similar or the same security issues, so they hardly understand each other in joint efforts to solve security issues.

Several ongoing activities on security solutions aim to integrate existing guidelines, best practices, security standards and existing solutions. The main information resources are the ISO/IEC 27000 series of standards, ENISA agency, NIST agency, InfoSec institute, SANS institute, national CERT organizations, different national IT Security guidelines (BSI, 2007; CNiL, 2010) and others. They are used as the basis for several integrated solutions and knowledge bases, such as the ontology of security metrics (Sajko et al., 2010), Common Body of Knowledge (Schwittek et al., 2012) and Security Ontology (Fenz et al., 2011). Additionally, there are several risk management tools that exist, such as the AURUM software tool based on the NIST SP 800-30 risk management standard (Ekelhart et al., 2009), the GSTool based on the German IT Grundschutz Manual (BSI, 2013), the EBIOS methodology tool based on the French EBIOS standard (ANSSI, 2013), the risk analysis based CORAS method (Lund et al., 2011) that partly supports the ISO/IEC 27001 standard, the risk based DDP tool supported technique for quantitative risk analysis reasoning method (Cornford et al., 2006) or the MOPM method based on combining the Analytic Hierarchy Process (AHP) and Particles Swarm Optimization (PSO) (Awad et al., 2011).

These solutions are often developed either for business and security managers or for security experts and technicians, and they mostly do not take into account human influence. Moreover, there is no overall, generally applicable solution to prove their productivity and quality, e.g., even some criticism towards ISO/IEC is highlighted (Beckers et al., 2012).

In this paper, we present an information security model based on an OWL ontology, an enhanced Evidential Reasoning algorithm and a simple reflex intelligent agent's algorithm. Knowledge base security ontology gives a logical basis for this model by defining descriptive formal knowledge on security issues (Gruber, 1995), while the enhanced ER algorithm is the mathematical evaluation algorithm of this model (Yang and Xu, 2002). The simple reflex intelligent agent's algorithm, as the decision supporting element for automated back coupling, should search through the ontology to find security critical elements or low security level subsystems (Russell and Norvig, 2010).

The main properties of this solution are aimed at: high flexibility and applicability to both different information solutions and different business organizations; upgradeability to be up to date in real time regarding security issues and new threats; and high versatility, taking into evaluation all possible aspects of security, e.g., network security, software and hardware issues, human factor, security policies and disaster recovery protocols.

Information security evaluation results gained with this model are as follows: overall grade on information system's security level; identification of low security level subsystems; and security critical elements of the evaluated information system. After determining the overall security level and identifying security critical elements of the evaluated system, it is left to business and security management to decide on necessary actions. Decisions on which security solution is the best for an evaluated business organization regarding ROI and business needs are left to the management.

We made three assumptions to build the proposed model. The first assumption was the consideration of the user as the constitutive part of the information system that will be evaluated. Because the user can significantly affect the overall systems security level (Solic et al., 2011), its behaviour or awareness regarding security issues has to be taken into evaluation. The second assumption was that the enhanced ER algorithm, which is developed for static and dynamic technical systems' state evaluations, can be used to evaluate users' behaviour (Solic et al., 2013). The third assumption was that, currently, looking from the information security perspective, data as written information is the universal currency and main asset in every business process (Haley, 2012). The third assumption makes the proposed model generally applicable.

Possible problems can be found in the quality of security ontology and subjective expert's assessment methodology. The first problem can be solved with ongoing work on building a common body of knowledge on security issues organized as ontology (Schwittek et al., 2012). The solution of the second problem is covered by using all properties of the enhanced ER algorithm, which is based on the Dempster–Shafer theory that mathematically addresses uncertainty and subjectivity (Yang and Xu, 2002).

Instead of focusing on known security threats and the identification of possible security breaches, the presented model searches for opened back doors and the smallest security critical elements of the examined information system and, by grading the overall security status and comparing it to referent values, gives a basis for decision on whether the security level should be improved. It also takes human impact into consideration, as humans are still the weakest link of an information security system (Sasse et al., 2001).

The proposed solution is applicable to differently sized business organizations as well as to small, standalone information systems, such as smart mobile phones. It can cover all possible aspects of security issues and can be highly up to date as long as the security ontology is well defined. This solution should be usable by both security experts and business managers because it tries to include both risk management and a technical approach towards security issues.

We applied the proposed model on a small business organization's information system. For testing purposes, we also used the standard qualitative risk assessment method on the same organization and compared the results.

The presented model aims to become the basis for a novel information systems security evaluation solution that should cover all possible information security issues.

In the next section, we discuss some related work, and, in Section 3, we present a detailed description of the proposed model design. In Section 4, we present usage of the proposed model and compare it with the qualitative risk assessment method. The conclusion and plans for further development are given at the end of this paper.

2. Background and comparison to related work

There are several Security Requirements Engineering (SRE) methods that support implementation of the ISO/IEC 27001 information security management standard, such as the goal oriented KAOS (Dardenne et al., 1993) and SecureTropos (Mouratidis and Giorgini, 2007), problem oriented method SEPP (Schmidt et al., 2011) and risk analysis based method CORAS (Lund et al., 2011). The most comparable SRE method with our presented model is, perhaps, the CORAS risk analysis method.

CORAS is also a model-based solution that uses either its customized language or UML for the representation of domain structure. This method relates assets and risks annotated with likelihoods to support quantitative reasoning in the identify–assess–control cycle of security risk analysis (Lund et al., 2011). However, likelihoods and their contributions remain fairly vague from a semantic standpoint.

The Defect Detection and Prevention (DDP) process is a principal tool under development as part of the NASA Failure Detection and Prevention spacecraft program. It is adapted for Information Security Risk Management as a tool supported technique for quantitative risk analysis and life cycle risk management (Cornford et al., 2006). The DDP process can be divided into three phases: determination of the goal, identification of possible obstacles that could get in the way and determination of countermeasures to achieve the defined goal. The tool has a somewhat smaller knowledge base made of trees of requirements, trees of potential failure modes and sets of PACTs (preventative measures, analysis, process controls and tests). Scoring the impact of failure modes on the requirements will result in a prioritized set of failure modes. The result is an optimally selected subset of PACTs to minimize residual risk, which is subject to the project resource constraints. Although this solution was not developed for information security risk management, it can be used in that manner. However, it is a process based solution with questionable quality of its knowledge base.

The GSTool is a software tool that supports users in preparing, administrating and updating IT security concepts that should meet the requirements of the German IT Grundschutz Manual (BSI, 2007, 2013). It is a comprehensive reporting system that provides support for the following tasks within the framework of security concepts: modelling, in accordance with IT Grundschutz system recording and structural analysis; application recording; implementation of safeguards; cost analysis; protection requirement determination; reporting; revision support; basic security check; and IT Grundschutz certificate. Quality of this solution depends on how well the IT Grundschutz Manual is kept up to date. Additionally, current information stands that technical support for this tool will be provided until the end of 2015.

The EBIOS software tool is developed by the Central Information Systems Security Division under governance of the French Network and Information Security Agency (FNISA) to support the EBIOS method based on ISO/IEC applicable standards (ANSSI, 2013). This tool helps the user to produce all risk analyses and management steps according to the five EBIOS phases and allows all of the study results to be recorded and the required summary documents to be produced. It provides risk identification, risk analysis, risk evaluation, risk assessment, risk treatment, risk acceptance and risk communication, among other risk management issues. The tool is an open source and free to use solution, but it is also only as good as its knowledge base.

The Multi Objectives Programming Methodology (MOPM), based on the Analytic Hierarchy Process (AHP) and Particles Swarm Optimization (PSO), combines the analytic hierarchy structure of risk assessment and comprehensive judgement according to the actual condition of the information system security (Awad et al., 2011). Additionally, the risk degree is a PSO estimation of the risk probability, risk impact severity and risk uncontrollability. This methodology is developed for risk assessment and condition evaluation of the information system security to become a supporting tool for decision makers, but it lacks a formally defined knowledge base.

The software tool based on the AURUM methodology looks the most similar to the presented model among the other analyzed solutions (Ekelhart et al., 2009). AURUM is based on the NIST SP 800-30 risk management process. It uses security ontology as a knowledge base, meaning that it incorporates existing best practice guidelines and information security standards to ensure up to date property that is based on the ongoing project of building a body of knowledge (Schwittek et al., 2012). The solution uses a Bayesian network for threat likelihood determination, calculating subjectivity into objectivity, offers some automatic support in decision making, considering multiple objectives, and provides gap analysis (Ekelhart et al., 2009). Regarding testing results obtained with the enhanced ER algorithm, this algorithm seems to be a better choice for the evaluation process and easier to apply onto an ontological structure than a Bayesian network. Another problem is that this solution does not support the evaluation of users' awareness impact on the system's security.

The conceptual model, based on the standard UML class diagrams, consists of the elaboration of hierarchical taxonomy of the terms within the defined information security policy domain. This model recognizes three key factors of information security policies: people, process and technology. The research goal is to encompass the influence of the contemporary environment on the information systems and other information security policy factors to construct a complete conceptual model (Klaic and Golub, 2013). This type of overall security ontology is still in the early development state but possibly usable as a knowledge base for the model presented in this paper.

A prototype of the users' awareness evaluation tool has several similarities to the presented model (Kruger and Kearney, 2006). It has a tree based logical structure, has an evaluation algorithm that takes into account weights regarding the importance of different system elements and can be extended to cover all of a system's security issues. However, it seems that it has not been developed further, lacks a knowledge data base and cannot calculate with subjectivity values.

Another comparable solution used for the evaluation of users' awareness and information security training is based on security ontology (Mangold, 2012). Perhaps this solution can be integrated into some previously described solutions, e.g., AURUM, to include the impact of users' behaviour in security

evaluation. However, this solution is in the early development phase and seems to lack an evaluation algorithm.

The basic difference between the analyzed solutions and our proposed model is that the other solutions are focused on information security from a risk management point of view regarding known and existing security threats, often lacking the impact of the level of users' security awareness, while the proposed model is based more on current technical and organizational security issues to cover all possible security critical elements, including the evaluation of users' behaviour and awareness (Solic et al., 2013). Our solution tries to include both risk management and a technical approach towards security issues; therefore, it should be of interest to both security experts and business managers. The proposed model gives a basis for decision makers to find the best security solutions regarding ROI and a particular business organization's needs.

Knowledge base that we built as OWL ontology is a major element of the proposed model. It can provide high flexibility and applicability to different information systems and business organizations; upgradeability to be up to date regarding current security issues and new threats; and high versatility, taking into evaluation all possible aspects regarding security issues, e.g., network security, software and hardware issues, human influence, security policies and disaster recovery plans. We used the enhanced Evidential Reasoning algorithm to calculate the overall grade of a system's security level. This algorithm is based on the Dumpster–Shafer theory and is well suited for calculations with expert's subjective judgements combining qualitative with quantitative evaluation grades. We also designed an algorithm for back coupling based on a simple reflex intelligent agent for results presentation and decision support.

3. Model elements

Some of the properties the presented model is aimed at are flexibility, wide applicability and upgradability, which are achieved by modularity. Security ontology is the logical foundation of the presented model, the enhanced ER algorithm is chosen for mathematical calculations and the simple reflex intelligent agent's algorithm is defined for automated back coupling reasoning (Fig. 1).

The major and the most important element for this proposed model's quality is Data Knowledge Base designed as an OWL security ontology. Knowledge built into this element relies on different security guidelines and information security standards. However, used ontology can easily be upgraded or changed for a different one in order to meet the highest information security standards. After making certain adjustments, this enhanced ER algorithm can be applied on an OWL security ontology in order to calculate Utility Number as an Overall Grade of system's security level.

We also designed an algorithm for back coupling based on a Simple Reflex Intelligent Agent. This element has the task of identifying and pointing out possible opened back doors by searching through ontology for information system elements with low evaluation grades and to present evaluation results.

3.1. *OWL ontology*

The aim of the ontology concept, in general, is the formal description of domain knowledge that is readable to both humans and machines for the purpose of knowledge sharing between software agents (Gruber, 1995; Russell and Norvig, 2010). OWL

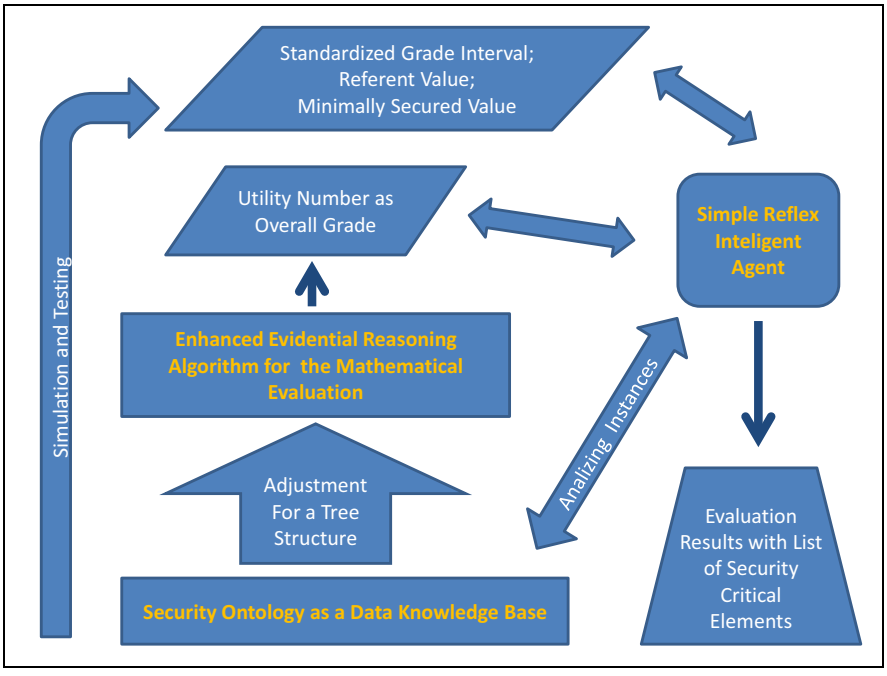

Fig. 1 – Diagram of the proposed model.

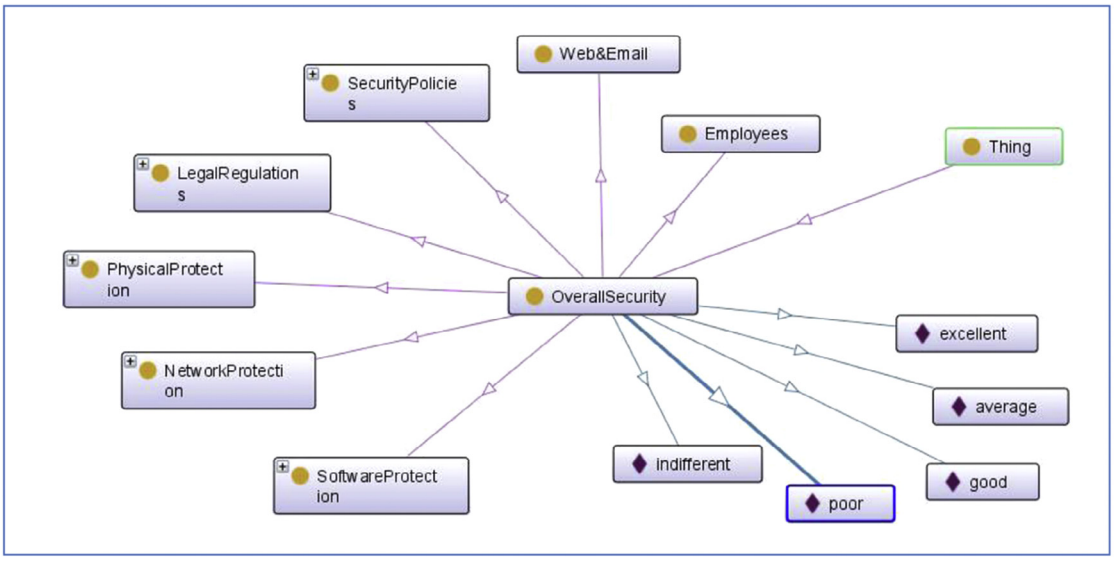

Fig. 2 – Example of a high level security ontology.

ontology is developed as the basis for semantic web (W3C, 2013a, 2013b). This type of ontology is the most frequently used type in the field of information science, especially for the description of security policies (Klaic and Hadjina, 2011). Ontology is reusable and easy to update (Noy and McGuinness, 2005). An additional reason for choosing OWL ontology as the logical foundation of the presented model is the ongoing work on developing overall and highly general security ontology (Fenz et al., 2011; Schwittek et al., 2012). However, in our work we have only used our own security ontology based on different security guidelines and information security standards.

The high level security ontology used in this paper is only an example of how it could be constructed; it is not a fixed or final version (Fig. 2). A more detailed part of security ontology is lower level security ontology, which presents file server protection (Fig. 3).

Detailed structure of the security ontology used in this work is presented in Table 2. In the proposed model it is possible

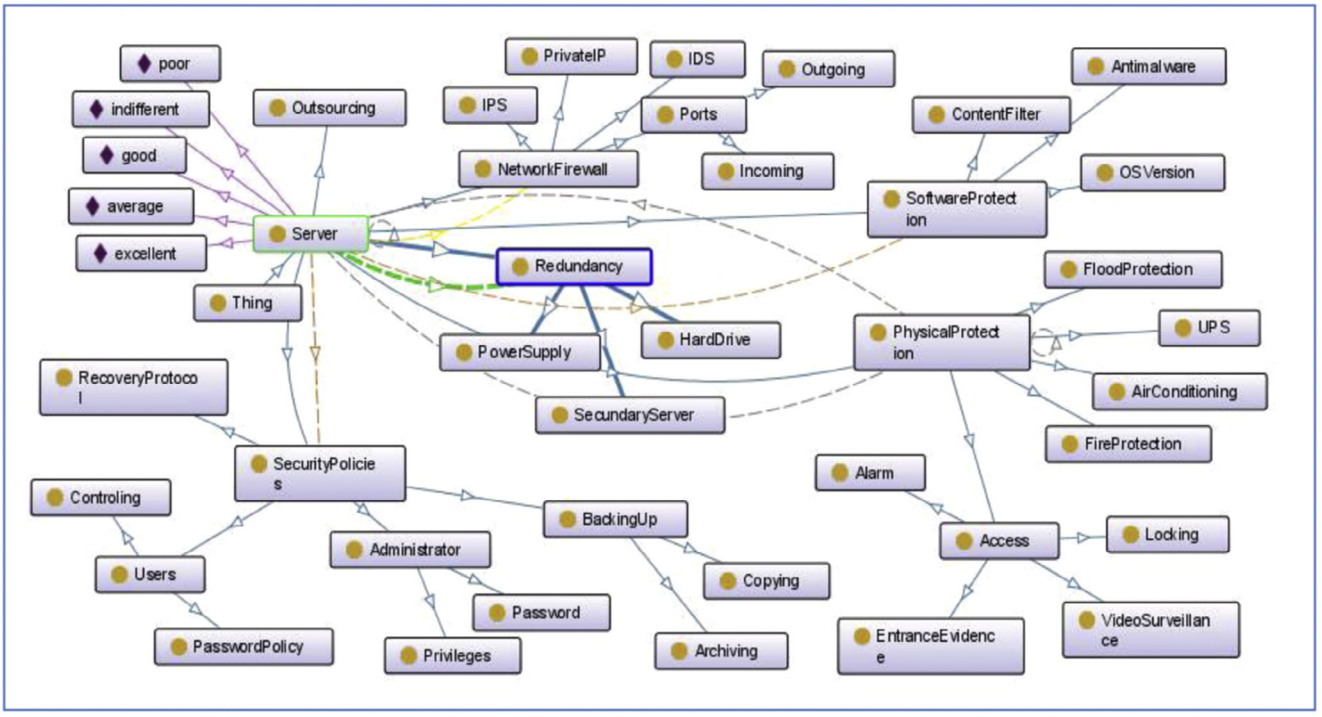

Fig. 3 – Example of a file server protection ontology.

to modify or to use existing security ontology or even to build a new one.

3.2. *Enhanced evidential reasoning algorithm*

The ER algorithm is well suited for dealing with a multiple criteria decision analysis (MCDA) problem, which considers the quantitative and qualitative measurements assessed using subjective judgements with uncertainties. This approach was introduced in the 1990s (Yang and Sen, 1994; Yang and Singh, 1994) and is based on the Dempster–Shafer (DS) theory (Dempster, 1967; Shafer, 1976), the decision making theory (Zhou et al., 2010) and the evaluation analysis model (Zhang et al., 1990). To use the ER algorithm to aggregate attributes of a multilevel structure, certain enhancement was done by proposing four synthesis axioms (Yager, 1987).

In our model, grading is mostly a subjective judgement made by security experts based on their knowledge and experience. Examples of qualitative measurement include grading password quality or using predefined grading scales for different guidelines and standards. Basic evaluation grades used in the proposed model create the distribution of six elements: grades from poor to excellent with uncertainty as the last element. Each grade is presented with a capital letter Poor, Indifferent, Average, Good or Excellent, while Uncertainty is presented with a capital letter H. Each grade has a related subjective belief presented as a proportion and shown as a decimal number in the brackets.

In the proposed model, basic attributes present basic subclasses in ontology. Because distributions are hard to compare, it is useful to calculate a single numerical value. The use of a utility number gives the overall grade of a system's security level, thus enabling a comparison between different systems or a comparison to the referent value (Jagnjic et al., 2004; Yang and Xu, 2002). The resulting grade, utility value is standardized on an interval between 0.00 and 1.00, and the utility interval is defined by the level of uncertainty. An example calculation for the quality of two different passwords presents a distribution of grades with related subjective beliefs and associated utility numbers with a utility interval (Table 1).

In this example, the first password was graded better by a security expert, while the second password received a lower and incomplete grade (with an uncertainty of 20%). The grade distribution for the password "*Ks1331sK*" means that 22% of a grade is rated by a security expert as Average, 33% is rated as Good and 45% is rated as Excellent. In comparison, the grade distribution for the password "*abcd123*" means that 20% of a grade is rated as Indifferent, 60% of a grade is rated as Average and 20% of a grade is rated as Uncertain. In both cases Utility numbers are a more reliable presentation of the total (overall) grade, making the comparison between the two easier.

Table 1 – Example calculation for a passwords' quality.

Password	Distribution of grades	Utility with uncertainty interval
Ks1331sK	A(0.22), G(0.33), E(0.45)	0.852
abcd123	I(0.20), A(0.60), H(0.20)	0.430 (0.330–0.530)

A more detailed explanation of the enhanced ER algorithm can be found as explained by Yang and Xu (2002). Some examples of the enhanced ER algorithm applied to technical systems include: the oil reserve forecast (Zhang et al., 2005), motorcycle evaluation (Yang and Xu, 2002), car industry (Liu et al., 2008), expert system (Beynon et al., 2001), knowledge reduction (Wu et al., 2005), risk analysis (Srivastava and Liu, 2003) and electric power grid evaluation (Jovic et al., 2004).

3.3. *Defined algorithm based on the simple reflex intelligent agent*

We defined algorithm for decision support and results presentation that is based on the simple reflex intelligent agent. This type of agent is well suited for the automated back coupling reasoning in the presented model. Regarding definition, an agent can be anything that perceives its environment through sensors and acts upon that environment through actuators; as the simplest type of agent, the simple reflex agent selects actions on the basis of its current perception, ignoring its historical data (Russell and Norvig, 2010).

Basically, this agent can be a security expert, i.e., a consultant that performs security evaluation of the information system's part of a business system. However, if automation is needed, the agent can be a small and simple software program with a defined algorithm (Fig. 4).

Agents inputs are: the referent value of the security level gained by simulation and testing; correction from the security expert regarding the security level needed for a particular business organization (particular ICT system); and utility evaluation grade calculated with the enhanced ER algorithm. An agent's action would be to search through instances in security ontology either directly or by using software ontology reasoners (Huang et al., 2008). Its output would be either a list of smallest security critical elements of the evaluated system, e.g., low level firewall or lack of antivirus, or less secured system parts, e.g. the whole WLAN or an entire HR department.

3.4. *Defining connectivity conditions between model parts*

To apply the enhanced ER algorithm on the information system's ontology, a description has to be organized in the superclass subclass hierarchical structure. To do so, these three conditions must be met (Solic et al., 2013):

1. the hierarchical structure should be an acyclic graph;
2. every direct relation should be a "one-to-one" or "one-to-many" relation;
3. crossing between classes should be reorganized.

If these conditions are not met in the ontology, one simple solution is to define additional classes to satisfy the acyclic property or to reuse some lower level classes by repeating them with the same grades and same degrees of belief to reorganize "many-to-many" relationships (Solic et al., 2013).

The utility number with a utility interval from the enhanced ER algorithm, which presents the security level grade, becomes one of the several inputs for the intelligent agent. To

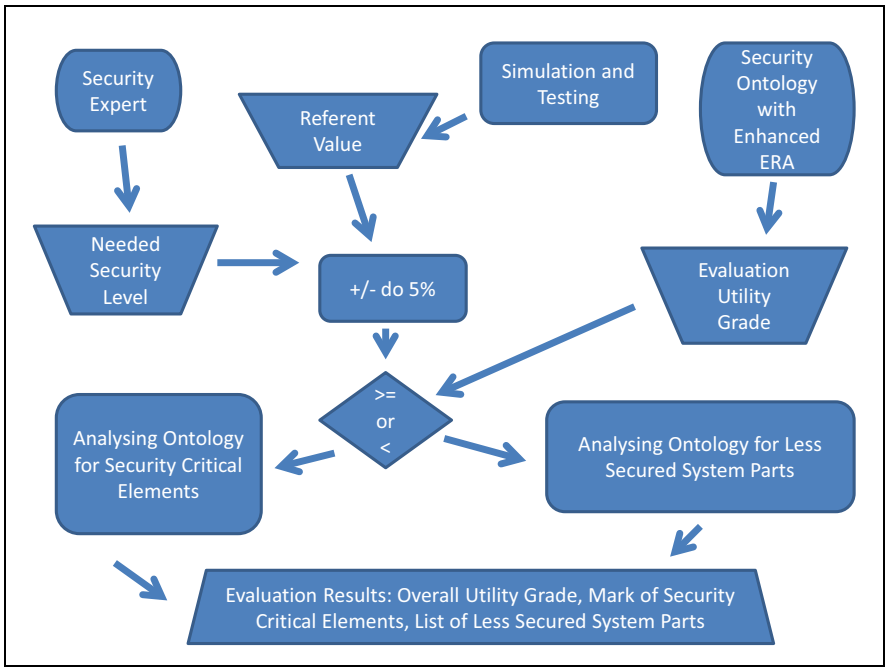

Fig. 4 – Defined algorithm for the simple reflex intelligent agent.

give control over security ontology to the intelligent agent, software reasoners built on tableau and predicate logic can be used (Huang et al., 2008). Another solution would be to build a software engine into the intelligent agent to search through an XML file because ontology can be printed out in XML form. If a human security expert is playing the role of the intelligent agent as the consultant leading the evaluation process, he/she can search through security ontology simply with a web interface because the OWL file is readable by web browsers.

4. Usage and preliminary model testing in real environment

To evaluate the presented model, we choose a small business company that agreed to participate in this research. Even though it was a rather small company with no more than 50 employees, it had 15 separate office locations and had recently adopted a plan to upgrade its IS structure. Three of those locations had an information subsystem connected to the company's information system, while another 7 still needed to be connected to the overall information system. Most of the information system's infrastructure was fragmented and built from obsolete technology, thus having urgent need for reengineering of the whole information system. For the purpose of presentation in this paper, we only evaluated the administrative business unit.

In this company, we made two parallel information security assessments. We applied our model to test it and also used the standard security risk assessment method to compare results. Both assessments included standard technical and organizational security issues (both digital and hard copy documentation) and also an examination of users' awareness and behaviour.

4.1. *Security state assessment using presented model*

The assessment process was guided by the proposed security ontology (Fig. 2), which did not need to be modified or adapted for the evaluated business organization.

The security expert in cooperation with a person in charge of company's information system grades each smallest segment of the examined system. These smallest segments are then presented as the smallest subclasses in the defined security ontology. Example in Table 2 can be: "Quality" of "Antivirus Software Protection" under "Network and Software protection" as a part of the high level security ontology in Fig. 2. Security expert gives subjective grade as distribution of five elements from Poor to Excellent (presented with capital letters: P, I, A, G, E) with the Uncertainty (capital letter H). In our example distribution of grades is made by 50% of grade Good and 50% of grade Excellent with ought Uncertainty: P(0.00), I (0.00), A(0.00), G(0.50), E(0.50), H(0.00).

Applying enhanced Evidential Reasoning algorithm on all three distribution grades regarding "Antivirus Software Protection" new distribution of grades is then calculated: P(0.154), I(0.154), A(0.00), G(0.154), E(0.539), H(0.00). The new distribution is one of the 14 attributes for calculating "Network and Software Protection" distribution of grades. New grade distribution equals: P(0.373), I(0.087), A(0.117), G(0.279), E(0.134) H(0.010) while the utility value equals U = 0.471 with the utility interval (0.466–0.476).

The overall utility grade with its respective utility interval is calculated in order to be able to compare different grade's distributions. The evaluation grade is standardized on an

Table 2 – Detailed calculation of the evaluation grades based on used OWL security ontology.

Information system's security ontology elements	Overall grade calculation	Utility values
Overall system's security	P(0.054), I(0.173), A(0.142), G(0.543), E(0.084), H(0.005)	0.687 (0.684–0.689)
Network and software protection	P(0.373), I(0.087), A(0.117), G(0.279), E(0.134), H(0.010)	0.471 (0.466–0.476)
Network administration quality	I(0.80), A(0.20)	
Defined security level with defined requirements	P(1.00)	
Network segmentation	P(1.00)	
Firewall	G(1.00)	
IDS	Outsourced	
IPS	Outsourced	
Ports	Outsourced	
Antivirus software protection	P(0.154), I(0.154), G(0.154), E(0.539)	
Quality	G(0.5), E(0.5)	
Upgrade regularity	E(1.0)	
Computer maintenance	P(0.5), I(0.5)	
Antispyware protection	Outsourced: G(1.00)	
Spam filters	Outsourced: G(1.00)	
Backup quality	P(0.90), I(0.10)	
Redundancy	P(0.90), I(0.10)	
Encryption	P(1.00)	
Protection of communication between Departments	A(0.50), G(0.50)	
Protection of communication with external businesses	A(1.00)	
Protection of mobile media	P(0.154), A(0.039), G(0.205), E(0.449), H(0.154)	
Notebook	G(0.5), E(0.5)	
Portable HDD	P(0.8), A(0.2)	
CD/DVD Media	Not evaluated	
USB memory	E(1.0)	
Mobile phone	G(0.5), E(0.5)	
Network access from home or business type	E(1.00)	
Physical protection	P(0.058), I(0.127), A(0.158), G(0.274), E(0.356), H(0.028)	0.734 (0.720–0.748)
Access control of employees	P(0.300), A(0.075), G(0.300), E(0.075), H(0.250)	
Towards file server	Not evaluated	
Towards each personal computer	G(0.8), E(0.2)	
Towards network	P(0.8), A(0.2)	
Access control of external associates	E(1.00)	
Towards file server	E(0.10)	
Towards each personal computer	E(0.10)	
Towards network	E(0.10)	
Video-surveillance system	P(0.262), A(0.246), G(0.164), E(0.328)	
Coverage	A(0.5), G(0.5)	
Night watch	P(0.8), A(0.2)	
Archive quality	E(1.0)	
Fire protection	G(1.00)	
Flood protection	G(0.70), E(0.30)	
Overheat protection	P(0.50), I(0.50)	
Robbery protection	A(1.00)	
Old equipment safe disposal	E(1.00)	
Security procedures	P(1.00)	0.350
Security policy	Not defined	
Quality		
Compliance		
Password policy	Not defined	
Quality		
Compliance		
Disaster recovery protocol	Not defined	
None-disclosure agreement with external businesses	Not defined	
Equipment inventory	Not defined	
Employee	Not defined	
Obligations included in employment contract		
Periodical education		
Warning system		
Defined network user's rights		
Termination period protocol		

(*continued on next page*)

Table 2 – (*continued*)

Information system's security ontology elements	Overall grade calculation	Utility values
System's paper elements	P(0.118), A(0.323), G(0.479), E(0.081)	0.707
Storage	A(0.70), G(0.30)	
Access control	P(0.50), A(0.50)	
Physical protection	P(0.154), A(0.423), G(0.269), E(0.154)	
Centrically organized	P(0.5), A(0.5)	
Fire protection	G(0.5), E(0.5)	
Flood protection	A(0.7), G(0.3)	
Old documents safe disposal	G(0.70), E(0.30)	
Documentation flow between departments	G(1.00)	
Legal regulations regarding information security	A(0.208), G(0.708), E(0.083)	0.799
Archiving	G(0.80), E(0.20)	
Compliance	A(0.50), G(0.50)	
Web site and email system	G(1.00)	0.850
Web site	Outsourced	
Email system	Outsourced	
Employee as ICT system's user	A(0.266), G(0.734)	0.770
Potentially risky behaviour	A(0.20), G(0.80)	
Knowledge and awareness	A(0.40), G(0.60)	

interval between 0.00 and 1.00, and the utility interval is defined by the level of uncertainty in the evaluation.

The overall evaluation grade of the information security status was U = 0.687 (0.684–0.689). Because the evaluation grade is standardized, a desirable grade should be at least greater than 0.80.

The evaluated business unit has a relatively well graded "Legal Regulations", "Employees' Awareness" and outsourced "Web and Email" of the information system (Table 2). A very low security evaluation grade is associated with "Network and Software Protection", meaning that the LAN protection is below average. Because the company has not developed "Security Procedures", which causes a lack in that subclass' evaluation, the evaluation grades were set at *poor*. Users of the business information system, i.e., the employees, were examined with a validated UISAQ questionnaire (Velki et al., 2014) and received a utility evaluation grade somewhat lower than desired (U = 0.77). With the used questionnaire, it was possible to evaluate separately users' behaviour and users' awareness of information security issues. Employees received a better grade regarding behaviour.

After applying the simple reflex intelligent agent's algorithm, several security critical elements were noted:

- quality of backup solution (under "Network and Software Protection") was extremely low (U = 0.035);
- there was no redundancy solution, encryption is not used, network segmentation does not exist and network security requirements are not defined;
- utility grade was *poor* (U = 0.350) for subclass "Security Procedures";
- utility grade was below average for subclass "Network and Software Protection" (U = 0.471 (0.466–0.476));
- utility grade was relatively low for subclass "System's Paper Elements" (U = 0.707);
- scepticism towards collocutor in subclass of users' "Knowledge and Awareness" was very low (U = 0.41);
- under subclass of users' "Potentially Risky Behaviour", several elements received low grades: using different passwords for accessing different systems (U = 0.43); for Administering personal computers at home (U = 0.43); and for locking on PCs when leaving the office table (U = 0.45).

Calculated evaluation utility grades of each system's segment (subclass) and detailed calculations from distribution of grades are presented in Table 2.

4.2. *Risk assessment using qualitative risk assessment method*

Risk assessment was carried out in the scope of the information security management system. Recommendations and practices for risk management of information security currently used are based on the ISO 27001:2013 standard and NIST 800–30 publication guidelines. Standard ISO27001 in the parts dealing with risk management references to ISO27005 which provides complete information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review. Family ISO27000 encompasses the entire information system security management, but it is also possible to restrict the process to a specific area. The standard is selected due to the comprehensiveness of actions in the desired scope. The methodology and procedures in assessing and managing risks are determined on the basis of family ISO31000 – Risk Management.

In this study were used practices that are described in the above standards. The methodology described in this paper is based on the overall management information systems and the associated risks.

The initial step in the evaluation is the definition of property within the scope and estimation of the asset value. The property is divided into categories and the value is estimated based on the qualitative impact that would cause the loss of some of the property characteristics. Properties of assets are confidentiality, integrity and availability. Every piece of property is evaluated regarding vulnerabilities and threats, which, in combination with one another, constitute the risks.

Risk management in information and communication systems is a process that includes the activity of risk assessment and mitigation of unacceptable risks to acceptable values or implementation of alternative methods of overcoming risks. Risks can be mitigated by implementing control measures, avoiding, transferring to a third party or acceptance. Acceptance of risk does not diminish the value of risk but appoints awareness and acceptance of the existence of irregularities that can lead to potentially risky situations. Risk management combines all of the activities and defines a repeating cycle in which all of the parameters are updated and new values are entered, as well as mutual combinations of parameters.

Risk assessment within selected areas of information security management may refer to more detailed issues. The implementation of the classic PDCA (Plan-Do-Check-Act) cycle would ensure a continuous process of risk management, which also ensures a high level of awareness within the organization. The intention of the ISO with Annex 2013 was to align all of the management standards to make them more compatible and enable the integration of management systems in an easier and more convenient way. The PCDA is still very much incorporated into ISO 27001 and most of the other standards, only now the cycle is not expressly displayed in the introduction of the standard, as was the case in the older revisions. The structure of the ISO standards and recognition of the PDCA cycle is as follows:

- the *Plan* phase, which includes clauses 4 (Context of the organization), 5 (Leadership), 6 (Planning) and 7 (Support);
- the *Do* phase, which includes clause 8 (Operations);
- the *Check* phase, which includes clause 9 (Performance evaluation);
- the *Act* phase, which includes clause 10 (Improvement).

Assessment results indicate the absence of policies that should regulate information security management as the biggest problem. The solution imposes the implementation of basic processes with the aim of preserving the properties of information assets.

The largest number of risks with high values is linked to force majeure or unintentional errors that are directly associated with a low level of awareness. The company has a low level of development of information security. Risk analysis shows that individual assessment of the property gives the same results as a consolidated approach. The company has no defined basic processes of information security management.

Organizational problems within the company are also the cause of many of the most prominent risks. The organization of information security is defined in many standards that manage an information system's governance. The implementation of the above standards ensures high quality security and risk management in information and communication systems.

The most significant identified risks are caused by the existence of significant vulnerabilities in the process:

- maintenance of infrastructure, including environment of information processing equipment;
- hardware maintenance;
- protection against unauthorized access;
- lack of staff.

Based on the recorded vulnerability, the assessment has identified a high probability of realization of the following threats:

- errors or degradation of equipment;
- unauthorized access to information;
- loss of authorized personnel.

Fig. 5 shows detailed results of the risk assessment method. The tool used for the assessment of these risks is configured so that the risks to the values of up to 6 are accepted (green color), and those over 6 are not eligible. Fig. 5 shows the mean values of the risks in the above areas. The methodology of risk management must be made in an organization that is applied, and as such needs to be conducted. Eligible risks indicated in the figure are the rule to be applied in general. Larger surface area covered by the curve represents a lower level of maturity.

Risk analysis is carried out at a very low level of information security management. Recorded risks point to the lack of important processes, and recommendations may indicate a need for the implementation of management information systems standards.

4.3. *Discussing compliance of both results*

In both assessment methods, i.e., standard qualitative risk assessment and the proposed model, evaluation is based on some grading scales. However, those scales are different; they grade similar but different things and therefore the resulting grades and sub grades are also different in subject. Both assessment methods have quantitatively measured qualitative security properties of an information system. Consequently, the assessment methods are not comparable when examining numeric results.

Therefore, we decided to compare conclusions that are noted in both assessments. This was sufficient for preliminary testing to gain first conclusions on the proposed model.

Comparing conclusions made with each of the methods, we concluded that the conclusion results are in congruence both in general conclusion and in pointing out some security critical issues. Detailed discussion of the conclusion results is as follows.

Both assessment methods noted the lack of some basic information system security elements. Comparing the results of both methods, compliance is evident in these processes:

- managing network-programming infrastructure;
- information security management;
- level of staff awareness.

Both assessment methods identified security problems with highest importance in the analyzed small business company. Both methods indicated the same problems but in different ways.

Maintenance of infrastructure and hardware, noted by risk assessment, is compliant with the proposed model's low grade for subclass "Network and Software Protection". It is more evident in pointing out the low quality of backup as one of the main security issues.

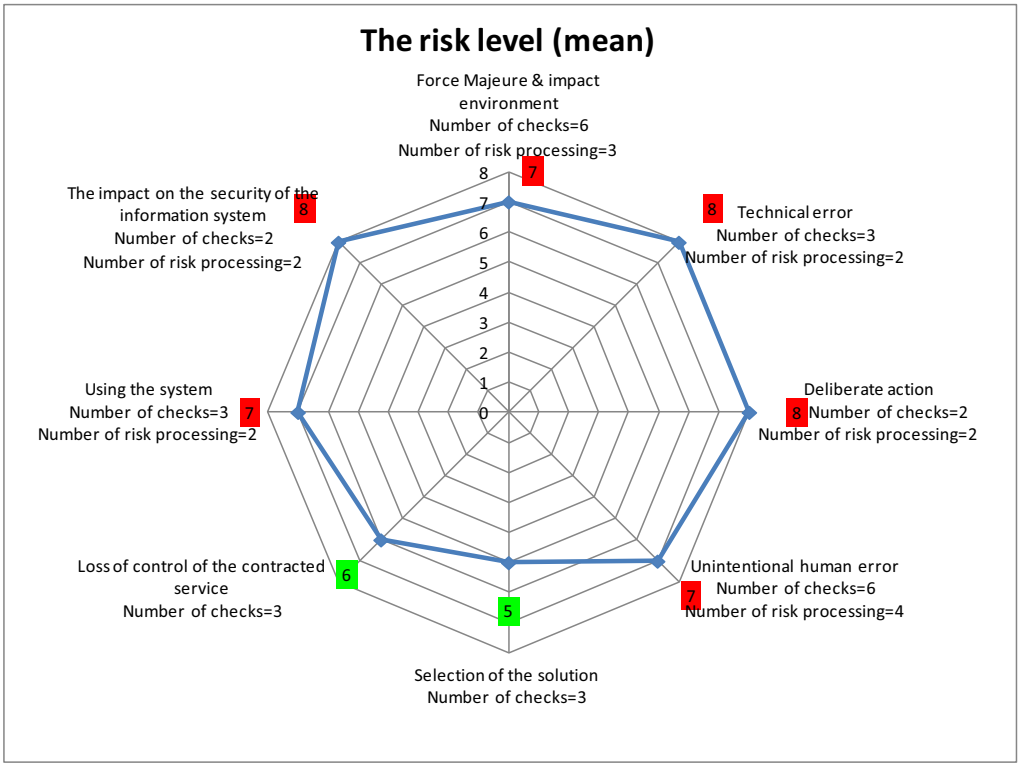

Fig. 5 – Risk assessment results. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

In addition, the lack of security policies and network system administrator noted by the presented model are compliant with the problem of information security management noted by the risk assessment method.

However, the presented model gives more detailed analysis on users' security awareness and behaviour. The low level of users' security awareness is noted in both assessments, but the presented model notes the existence of good physical protection and lack of additional control over users' malicious or accidental risky behaviour.

Both methods indicate the same problem, which could be solved by the implementation of proposed measures to mitigate risk.

In general, the conclusion results gained by the presented model are more detailed and cover more potential information security issues, while the results gained by the risk assessment method only note what might happen.

These preliminary model testing results look promising and confirm that the proposed model detects potential information security issues. Preliminary testing results also confirm that the integration of OWL security ontology and the evidential reasoning approach with an intelligent agent can be a good basis for an information security software tool. However, more testing is needed, development of the integral software tool should be made and referent values should be defined. Although, the assessment process seems to be correct, while the quality of the entire security assessment process greatly depends on the quality of security ontology.

5. Conclusion and future work

Preliminary results gained by applying the proposed model in a real environment and compliance of those results and results gained with the standard qualitative risk assessment method implicate that the aim is achieved. The presented model could be the basis for a novel information system's security evaluation software tool, covering a wide range of all possible information security issues from different aspects, including network, software and physical protection, human influence and organizational security policies.

The presented model is based on a knowledge data base modelled with OWL ontology, uses an enhanced Evidential Reasoning algorithm for calculations and has a defined algorithm based on a simple reflex intelligent agent as the decision supporting element. Properties of the presented model supervene from properties of its building elements. Some of those properties include: high flexibility and applicability to both different information systems and different business organizations; upgradeability to be up to date in real time regarding security issues and new threats; and high versatility, taking into evaluation all possible aspects regarding security issues, e.g., network security, software and hardware issues, human factor, security policies and disaster recovery plans. Our solution tries to include both risk management and a technical approach towards security issues; therefore, it should be of interest to both security experts and business managers.

A few assumptions were made when developing the presented information security model: the user of the information system is considered as a constitutive part of the used system; the enhanced ER algorithm can be used to evaluate users' behaviour; information is today's main asset; and ongoing work on building general security ontology will produce an up to date knowledge base.

More testing should be done to define more precise referent values (e.g., minimal secure level, average security level and correction interval). There exists a high amount of subjective judgement in the evaluation process, but the enhanced ER algorithm has proven to be a good choice because it is based on the Dempster–Shafer theory. Additionally, weighting attributes defined in the ER algorithm are not used in this work but can be practical in defining the different importance and impact of basic system elements on the overall system's security level.

Plans for future work include further model testing by evaluating the security of a business organization's information system using one of the existing OWL security ontologies. The quality of the presented model directly depends on the quality of OWL security ontology as its knowledge base. Today, OWL ontology modelling is common in the information security field and there is an ongoing effort to build a general overall ontology concerning information security; this is one of the reasons to continue this work to develop an integral software tool.

Another plan for further development is to build a software engine for the intelligent agent to search through an XML file because ontology can be printed out in XML form to automate an intelligent agent's reasoning.

It seems that the presented model, if developed as an integral software tool, could become a good information security evaluation tool that is useful to both security experts and business managers. That solution would be generally applicable to different types of information systems, covering both organizational and technical security issues.

Acknowledgments

Great appreciation goes to Professor Franjo Jovic for his very useful suggestions and guidance through this research. Our appreciation also goes to several nameless reviewers for their constructive criticism and suggestions.

REFERENCES

ANSSI. Software tool EBIOS. <http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/>; 2013.

Awad GA, Sultan EI, Ahmad N, Ithnan N, Beg AH. Multi-objectives model to process security risk assessment based on AHP-PSO. Mod Appl Sci 2011;5(3):246–50.

Beckers K, Faßbender S, Heisel M, Schmidt H. Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation, Proc. 7th international conference on availability, reliability and security (ARES '12). 2012. p. 242–8. doi:10.1109/ARES.2012.35.

Beynon M, Cosker D, Marshall D. An expert system for multi-criteria decision making using Dempster–Shafer theory. Expert Syst Appl 2001;20(4):357–67.

BSI. Federal office for information security IT security guidelines. Bonn. <https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html>; 2007.

BSI. Software tool GSTool. <https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzGSTOOL/itgrundschutzgstool_node.html>; 2013.

CNiL. Security of personal data. France. <http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf>; 2010.

Cornford SL, Feather MS, Hicks KA. DDP: a tool for life-cycle risk management. IEEE Aerosp Electron Syst Mag 2006;21(6):13–22. doi:10.1109/MAES.2006.1662004.

Dardenne A, van Lamsweerde A, Fickas S. Goal-directed requirements acquisition. Sci Comput Program 1993;20(1–2):doi:10.1016/0167-6423(93)90021-G.

Dempster AP. Upper and lower probabilities induced by a multivalued mapping. Ann Math Stat 1967;38(2):325–39.

Ekelhart A, Fenz S, Neubauer T. AURUM: a framework for information security risk management, Proc. 42nd Hawaii international conference on system sciences (HICSS '09). 2009. p. 1–10, doi:10.1109/HICSS.2009.82.

Fenz S, Parkin S, van Moorsel A. A community knowledge base for IT security. IEEE ITPro 2011;13(3):24–30. doi:10.1109/MITP.2011.35.

Gruber TR. Toward principles for the design of ontologies used for knowledge sharing. Int J Hum Comput Stud 1995;43(4–5):907–28.

Haley K. Information robbery: the 2011 internet security threat report, InfoSec Today. <http://www.infosectoday.com/Articles/Information_Robbery.htm>; 2012.

Huang T, Li W, Yang C. Comparison of ontology reasoners: racer, pellet, fact++, American Geophysical Union, fall meeting, abstract #IN13A-1068. 2008.

Jagnjic Z, Slavek N, Blazevic D. Condition based maintenance of power distribution system, Proc. EUROSIM. 2004. p. 13–14.

Jovic F, Filipovic M, Blazevic D, Slavek N. Condition based maintenance in distributed production environment. Mach Eng 2004;4(1–2):180–92. doi:10.1023/B:ISFI.0000005651.93751.4b.

Klaic A, Golub M. Conceptual modeling of information systems within the information security policies. J Econ Bus Manage 2013;1(4):371–6.

Klaic A, Hadjina N. Methods and tools for the development of information security policy, Proc. IEEE 34rd MIPRO. 2011. p. 1532–7.

Kruger HA, Kearney WD. A prototype for assessing information security awareness. Comput Secur 2006;25(4):289–96.

Liu X-B, Zhou M, Yang J-B, Yang S-L. Assessment of strategic R&D projects for car manufacturers based on the evidential reasoning approach. Int J Comput Intell Syst 2008;1(1):24–49. doi:10.2991/ijcis.2008.1.1.3.

Lund MS, Solhaug B, Stølen K. Model-driven risk analysis: the CORAS approach. Springer-Verlag; 2011. doi:bfm:978-3-642-12323-8/1.

Mangold LV. Using ontologies for adaptive information security training, Proc 7th international conference on availability, reliability and security (ARES '12). 2012. p. 522–4, doi:10.1109/ARES.2012.52.

Mouratidis H, Giorgini P. Secure tropos: a security-oriented extension of the tropos methodology. Int J Softw Eng Knowl Eng 2007;17(2):285–309.

Noy NF, McGuinness DL. Ontology development 101: a guide to creating your first ontology. Stanford University; 2005.

Russell S, Norvig P. Artificial intelligence, a modern approach. 3rd ed. Pearson; 2010. p. 46–50.
Sajko M, Hadjina N, Pesut D. Multi criteria model for evaluation of information security risk assessment methods and tools, Proc. IEEE 33rd MIPRO, 2010. p. 1215–20.
Sasse MA, Brostoff S, Weirich D. Transforming the "weakest link" – a human/computer interaction approach to usable and effective security. J BT Technol J Arch 2001;19(3):122–31.
Schmidt H, Hatebur D, Heisel M. Ch. 3: a pattern- and component-based method to develop secure software. In: Mouratidis H, editor. Software engineering for secure systems: academic and industrial perspectives. IGI Global; 2011. p. 32–74.
Schwittek W, Schmidt H, Beckers K, Eicker S, Faßbender S, Maritta H. A common body of knowledge for engineering secure software and services, Proc. 7th international conference on availability, reliability and security (ARES '12). 2012. p. 499–506.doi:10.1109/ARES.2012.31.
Shafer G. A mathematical theory of evidence. NJ, US: Princeton University Press; 1976.
Solic K, Sebo D, Jovic F, Ilakovac V. Possible decrease of spam in the email communication, Proc. IEEE 34rd MIPRO. 2011. p. 1512–15.
Solic K, Jovic F, Blazevic D. An approach to the assessment of potentially risky behavior of ICT systems' users. Tehn Vjesn 2013;20(2):335–42.
Srivastava RP, Liu L. Applications of belief functions in business decisions: a review. Inf Syst Front 2003;5(4):359–78.
Velki T, Solic K, Ocevcic H. Development of users' information security awareness questionnaire (UISAQ) – ongoing work, IEEE Proc. 37th MIPRO2014/ISS. 2014. p. 1564–8.
W3C OWL web ontology language overview. <http://www.w3.org/TR/owl-features/>; 2013a.
W3C OWL web ontology language guide. <http://www.w3.org/TR/owl-guide/>; 2013b.
Wu W-Z, Zhang M, Li H-Z, Mi J-S. Knowledge reduction in random information systems via Dempster–Shafer theory of evidence. Inf Sci 2005;174(3–4):143–64. doi:10.1016/j.ins.2004.09.002.
Yager RR. On the Dempster-Shafer framework and new combination rules. Inf Sci 1987;41(2):93–137. doi:10.1016/0020-0255(87)90007-7.
Yang J-B, Sen P. A general multi-level evaluation process for hybrid MADM with uncertainty. IEEE Trans Syst Man Cybern 1994;24(10):1458–73. doi:10.1109/21.310529.
Yang J-B, Singh MG. An evidential reasoning approach for multiple attribute decision making with uncertainty. IEEE Trans Syst Man Cybern 1994;24(1):1–18. doi:10.1109/21.259681.
Yang J-B, Xu D-L. On the evidential reasoning algorithm for multiple attribute decision analysis under uncertainty. IEEE Trans Syst Man Cybern 2002;32(3):289–304. doi:10.1109/TSMCA.2002.802746.
Zhang X-D, Zhao H, Wei S-Z. Research on subjective and objective evidence fusion method in oil reserve forecast. J Syst Simul 2005;17(10):2537–40.
Zhang ZJ, Yang J-B, Xu D-L. A hierarchical analysis model for multiobjective decision making, analysis, design and evaluation of man–machine systems. Oxford, UK: Pergamon; 1990. p. 13–18.
Zhou M, Liu X-B, Yang J-B. Evidential reasoning-based nonlinear programming model for MCDA under fuzzy weights and utilities. Int J Intel Syst 2010;25(1):31–58. doi:10.1002/int.20387.

Krešimir Šolić received his Ph.D. in 2013 on the subject of Computer System's Security modeling at University of Osijek, Faculty of Electrical Engineering. He is CCNA Cisco certified network system engineer. As a IAESTE exchange student he worked at Ericson AB, Gothenburg. Today he is working at Faculty of Medicine as senior researcher giving lectures on subjects regarding biomedical statistics. His research interests include information security problems with focus on user's awareness and behaviour. Dr. Solic was a student member of IEEE, is a member of Croatian Society for Medical Informatics and of Croatian Society for Biostatistics.

Hrvoje Očevčić received his Ph.D. degree in 2015 on the subject of risk assessment methodology from Faculty of Electrical Engineering, Osijek, Croatia. He is currently employed as a senior internal auditor of information systems at Hypo Alpe-Adria-Bank. He deals with information security and risk assessment of information systems. He has published several papers in various international journals and conferences. His research interests include risk assessment, business continuity management, information classification, incident management and generally information security. He is currently working on completing of doctoral thesis on the topic of decision support systems in the management of information systems.

Marin Golub received his Ph.D. degree in 2001 on the subject of parallel genetic algorithms. He is associate professor at the Department of Electronics, Microelectronics, Computer and Intelligent Systems. He participated in six projects, five as a project member. He has served as a reviewer for several international journals and conferences; and supervised several doctoral and many graduate theses. He is member of the project "Optimization of renewable electricity generation systems connected in a microgrid" and Technology (COST) project "Trustworthy Manufacturing and Utilization of Secure Devices". His current research collaborators include Digital Security group, Faculty of Science, Radboud University Nijmegen.