

Grubor, Gojko; Barać, Ivan; Simeunović, Nataša; Ristić, Nenad

**Article**

## Achieving Business Excellence by Optimizing Corporate Forensic Readiness

Amfiteatru Economic Journal

**Provided in Cooperation with:**

The Bucharest University of Economic Studies

*Suggested Citation:* Grubor, Gojko; Barać, Ivan; Simeunović, Nataša; Ristić, Nenad (2017) : Achieving Business Excellence by Optimizing Corporate Forensic Readiness, Amfiteatru Economic Journal, ISSN 2247-9104, The Bucharest University of Economic Studies, Bucharest, Vol. 19, Iss. 44, pp. 197-214

This Version is available at:

<https://hdl.handle.net/10419/169065>

**Standard-Nutzungsbedingungen:**

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

**Terms of use:**

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*



<http://creativecommons.org/licenses/by/4.0/>

## ACHIEVING BUSINESS EXCELLENCE BY OPTIMIZING CORPORATE FORENSIC READINESS

**Gojko Grubor<sup>1</sup>, Ivan Barać<sup>2</sup>, Nataša Simeunović<sup>3\*</sup> and Nenad Ristić<sup>4</sup>**  
<sup>1)3)4)</sup> *Sinergija University, Bijeljina, Bosnia and Herzegovina*  
<sup>2)</sup> *Singidunum University, Beograd, Serbia*

**Please cite this article as:**

Grubor, G., Barać, I., Simeunović, N. and Ristić, N., 2017. Achieving Business Excellence by Optimizing Corporate Forensic Readiness. *Amfiteatru Economic*, 19(44), pp. 197-214

**Article History:**

Received: 29 September 2016  
 Revised: 18 November 2016  
 Accepted: 15 December 2016

### Abstract

In order to improve their business excellence, all organizations, despite their size (small, medium or large one) should manage their risk of fraud. Fraud, in today's world, is often committed by using computers and can only be revealed by digital forensic investigator. Not even small or medium-sized companies are secure from fraud. In the light of recent financial scandals that literary demolished not just economies of specific countries but entire world economy, we propose in this paper an optimal model of corporate computer incident digital forensic investigation (CCIDFI) by using adopted mathematic model of the *greed* MCDM – multi-criteria decision-making method and the *Expert Choice* software tool for multi-criteria optimization of the CCIDFI readiness.

Proposed model can, first of all, help managers of small and medium-sized companies to justify their decisions to employ digital forensic investigators and include them in their information security teams in order to choose the optimal CCIDFI model and improve forensic readiness in the computer incident management process that will result with minimization of potential losses of company in the future and improve its business quality.

**Keywords:** computer incident; forensic readiness; forensic alternatives; forensic criteria; greed multi-criteria method; *Expert Choice* evaluation.

**JEL Classification:** C39, G32, M15

### Introduction

In the last few years, cyber threats have become more sophisticated with blended diversified zero day attacks and they practically make ineffective the current container type security position (Casey, 2011; Choo, 2011; FireEye, 2013). Traditional reactive security systems (ISO/IEC 27001:2013) can no longer prevent many computer incidents (CIs). These risks can be mitigated by reducing the opportunities for cybercrime occurrence, making cybercrime

\* Corresponding author, **Natasa Simeunovic** – nsimeunovic@sinergija.edu.ba.

more difficult to commit and by increasing the likelihood of cybercrime detection and increasing the punishment associated with committing cybercrime (Choo, 2011).

Risk management can be a very helpful tool for companies in achieving sustainable competitive advantage. By implementing CI management, as the element of the overall process of managing risk of fraud, organizations can increase trust level from their shareholders, investors, audit committees, board members, management and society as whole. How to assess and manage risk is well described by Damodaran (2007), Giles (2012), Gibson (2014) and Wu, Chen and Olson (2014). Before defining proactive programs to prevent fraud, especially one which occurs in form of computer incident, it is necessary to understand fraud theory, its schemes and many other facts about fraud in order to make good fraud risk assessment so that digital forensic investigator would be better prepared to detect fraud (Vona, 2012).

Currently, some advanced forensic techniques, such as the unified social graph-based text mining framework to identify digital evidence from chat log data providing algorithms to identify key-terms representing the interests of users, key-users, and key-sessions, etc. can be used (Anwar and Abulaish, 2014). Apparently, for most effective CI management, some automatic forensic tool to image and analyze the data in real time should be used. However, such an automatic DF investigation and analysis tool requires more research and experiments in the future. In this paper, the authors propose a greed multi-criteria method to choose an optimal CCIDFI model in order to increase forensic readiness and mitigate risk of possible corporate fraud which can affect deeply (Dyck, Morse and Zingales, 2013) on achieved business excellence of company.

The article is organized as follows. Literature review of the most relevant findings regarding CI management and adopted MCDM and MCDA methods is given in the first section. Next section explains research methodology presenting the theoretical models, data and approach used in empirical analysis. Section 3 present results and provide discussion, while conclusions are given in the last section.

## **1. Literature review**

Proactive network security, including intrusion detection (Kaufman, 2012) and protection systems (IDPSs), strong monitoring, and logging security relevant events from all active network and network security devices into a centralized log server, can provide better network security (Bradford and Hu, 2005; Scarfone and Mell, 2007; Zimmerman, 2010; Alharbi, et al., 2012; Grubor and Njeguš, 2012). In the environment of highly sophisticated threats, high speed changes in attack method and the diversification of vulnerability detection and exploitation tools, even proactive security systems cannot provide protection. Therefore, some predictive (smart) security systems, such as the system of the so called digital ants (Haack, et al., 2011), detecting different types of malware breaking into a computer network over the Internet can be used.

Physical and computer security over assets, records and information present a key aspect of fraud prevention (Giles, 2012). New technological trends are very important, in fact, technology is the key to the success and support which can be exploit for business excellence of organizations (Uhl and Gollenia, 2016). In many companies there is no forensic capacity due to the lack of expensive technology and competent digital forensic investigators. Therefore, choice of the optimal model of corporative computer incident digital forensic

investigation (CCIDFI) recourse becomes a natural improvement of the CI management process.

A proactive forensic network, in the case of computer incidents, can make digital forensic (DF) investigation and later analysis much easier (Gorzalak, et al., 2011). If there is a huge volume of data that should be analyzed, a distributed digital forensic analysis model can be applied (Martini and Choo, 2014). In addition to the few papers published in this area, some authors (Martini and Choo, 2014) describe in detail the advantages of distributed file system forensics, providing better cost-effectiveness and efficiency for the DF analysis.

As CI management is one of the key strategies in mitigating information security risks, other authors (Ab Rahman and Choo, 2015) have proposed a conceptual cloud incident handling model including computer incident handling; and digital forensics and the capability maturity model for services (Team C.P., 2010) to more effectively handle incidents in the cloud. Generally, integration of the DF investigator into the information security team enables easier later investigation of the computer incident (Kent, et al., 2006). In the case of computer incident, many organizations try to identify the type of incident and recover systems by their own resources. Traditional Corporate Computer Incident Digital Forensic Investigation (CCIDFI) is typically performed by a hired, quite expensive, DF investigator acting as a consultant (Casey, 2011; Steel, 2006). If the attacked computer system cannot be turned off for any reason, a dynamic model of the live digital forensic can be used (Jones, Bejtlich and Rose, 2005). Moreover, if the DF investigator cannot approach the attacked server, for any reason, a technique of more expensive ethical hacking can be applied to remotely access the server and to take images of the HD (Hard drive), RAM (Random Access memory) and network card using a virtual snapshot tool (e.g. Hyper V in Microsoft Server 2012 R2).

In the area of Multiple-Criteria Decision Making (MCDM) and Multiple-Criteria Decision Analysis (MCDA) a variety of approaches and methods have already been published. Many of them have been developed and implemented by specialized decision-making software (Weistroffer, Smith, and Narula, 2005). Some of the MCDM methods have been comparatively studied in the book by Triantaphyllou (2013). Review of the available MCDM methods is completed in the work by Greco, Figueira and Ehrgott (2005). Generally, the MCDM problem can be represented in the criterion space or in the decision space. However, if different criteria are combined by weighted linear functions, it is also possible to represent the problem in the weight space.

Some methods require information on the decision makers' preferences at the beginning of the MCDM process. This approach is called as prior articulation of preferences that transforms the MCDM analysis into a single criterion problem (Keeney and Raiffa, 1993). Many methods, such as those based on estimating a value function or using the concept of outranking relations, or analytical hierarchy process, and some decision rule-based methods, have tried to solve MCDM evaluation problems using interactive progressive articulation of preferences throughout the solution process (Geoffrion, Dyer and Feinberg, 1972; Köksalan and Sagala, 1995; Köksalan Wallenius, and Zionts, 2011).

The authors of this paper choose the greed MCDM methods suggested by Žižović, et al., (2014) and a new distance based approach to the MCDM problem suggested in Salabun (2015) as a new, integrated approach to decision making regarding forensic readiness in business environment.

## 2. Methodology

### 2.1 Functional model of the corporative DF investigation

The functional model of the CCIDFI process should include the same principles, procedures, tools and techniques as those in the law enforcement DF investigation process, with the exception of arresting and sanctioning the attackers. The choice of the optimal CCIDFI process is closely related to the CI management process in companies. Currently, the first response to the computer incident is typically reactive in small and medium private companies. It focuses on re-establishing the information security system, patching vulnerabilities, removing malicious activity, recovering files and the ICT (Information Communication Technology) system, and reporting them to management (Nikkel, 2014). As CI is becoming more complex and typically involves multiple organizations, there is a growing need for CCIDFI readiness as a fundamental part of the CI management process. This CCIDFI readiness should include conceptual models, legal issues, and DF standard operating procedures (SOPs), creating international standards for evidence exchange, and developing technical capabilities for acquisition and analysis of digital evidence (DE) across multiple jurisdictions (Nikkel, 2014). Therefore CCIDFI readiness is a crucial part of security risk management, reducing both the costs of CI response and DF investigation (Nikkel, 2014). Depending on the size, companies can have different capacities for CCIDFI readiness with regard to staff competency and the technologies used. The role of the CCIDFI investigator and analysts in a security team could be summarized as follows:

- *First response to the computer incident* and documenting the original state of the attacked computer system to provide authenticity of the digital data (DD), determine the type of the CI, and prevent escalation of the attack.
- *Organizing and leading the security team* in the CI or computer crime DF investigation, providing DD integrity and documenting on each and all activities.
- *Applying SOPs* to access the attacked computer, taking physical acquisition and forensic images of all the suspect media using writing blockator.
- *Collecting all of the relevant DD* from the forensic images, recovering as much DD as possible and creating a time line of the attack from the log files of the network and security devices in the logical acquisition phase.
- *Analyzing DE traces* from the DD sources and constructing legally admissible DE.
- *Participating in the interrogation* of the suspected interior attackers or eyewitnesses.
- *Reconstructing the attack* by integrating digital and physical evidence, and reporting them to the manager for further steps – to involve law enforcement or not, depending on its impact on the company's image.

A competent CCIDFI team can provide valid forensic data for the law enforcement investigator that can cast doubt on the DE's integrity. Therefore, rigorous documentation of any activities in the CCIDFI process and DE handling must be undertaken for them to be accepted by law enforcement investigators and the DE admitted by judges. As adequate CCIDFI readiness is mainly costly, a team of computer science specialists usually leads the CI investigation and sometimes it can be supported by hired DF investigators as consultants. In this article, the authors suggest the use of the *greed MCDM* method as the

optimal CCIDFI model. In a case study, the proposed method is evaluated using the interactive software tool, *Expert Choice*, to help companies to strengthen their forensic readiness using an optimal or set of optimal CCIDFI model solution alternatives. The results are analyzed in the evaluation section.

## 2.2 Mathematical model of the greed MCDM method

Any multiple-criteria evaluation problem consists of a limited number of alternatives that must be known before starting of the solution process. Each of the alternatives can be represented by its performance, using multiple criteria or objectives. The criteria can be based on intuition or some other methods and their consequences could be very high. In making the decision to choose an optimal CCIDFI model, there are complex multiple criteria and multiple parties involved, such as the DF analyst, prosecutor, judge, victims and attacker that could be deeply affected by the consequences of the CCIDFI results. In the MCDM methods any problem should be properly structured and each chosen alternative explicitly evaluated against multiple criteria. The cost is one of the main criterion for the choice of the CCIDFI model, as in many MCDM methods, too. Some other criteria of the CCIDFI process quality, such as client satisfaction or digital evidence admissibility by judge that could be in conflict with the cost should be considered carefully. Therefore, there is no unique optimal solution due to more than one criterion in the CCIDFI model. It is necessary to choose the most preferred alternative from the available set or to group alternatives into a small set of different preferences, or a set of indifferent or non-dominated solutions. To help decision maker focus on the best alternative from the large set of indifferent solutions, some tools and criteria trade-off are needed (Keeney and Raiffa, 1993).

The MCDM problem may be defined as a process of finding the best alternative or a set of good alternatives for a decision maker. In this article, the MCDM analysis of the determined CCIDFI alternatives against given criteria is undertaken, based on the *greed method of MCDM* suggested by Žižović, et al. (2014). This method is based on calculating the distance of the given alternative,  $A_i$  from the hypothetical best alternative,  $A^*$ , and the hypothetical worst alternative,  $A_*$ . In this calculation, a number of parameters such as functional value of the criteria and functional description of the alternatives have to be considered. One alternative is better than another if it is closer to the hypothetical best alternative,  $A^*$ , and further from the hypothetical worst alternative,  $A_*$ .

Let us have a set of alternatives,  $A = \{a_1, a_2, \dots, a_m\}$  that is evaluated against a set of criteria,  $C = \{c_1, c_2, \dots, c_n\}$ . The criteria from the given set do not have the same value, therefore a weighted factor,  $z_k \in (0,1]$  is associated with each of the criteria  $c_k$ ,  $k \in \{1, 2, \dots, n\}$ . Here, the weight factor means the level of the criterion value for evaluation of each alternative in the given set of alternatives. Then, each criterion  $c_k$ ,  $k \in \{1, 2, \dots, n\}$  should be associated with a function  $Z_k : A \times A \rightarrow [0, +\infty)$  that measures the level of the value differences among the alternatives. The  $Z_k$  function associates each pair of alternatives  $a_i, a_j \in A$ , with a non-negative number  $Z_k(a_i, a_j)$  that represents the key performance indicator (KPI) of the  $Z_k$  function. For simplicity, for each  $i \in \{1, 2, \dots, m\}$ , let alternative  $a_i$  be represented as the

arranged  $n$ -tuple  $a_i = (a_{i1}, a_{i2}, \dots, a_{in})$ , or its equivalent  $a_i = (a_{ik})_{k=1}^n$ , where each coordinate  $a_{ij}$ , for  $j \in \{1, 2, \dots, n\}$ , is a non-negative real number that represents the degree of fulfilment of the criterion  $c_j$ . Then, the two new sets of the hypothetical alternatives  $\bar{A}$  and  $\underline{A}$  are constructed for further calculation. Thus, for a given set of alternatives  $A = \{a_1, a_2, \dots, a_m\}$ , the sets of alternatives  $\bar{A}$  and  $\underline{A}$  are defined as follows (Žižović, et al., 2014):

$$\bar{A} = \left\{ (\max_{i \in J} a_{ik})_{k=1}^n \mid J \in P(\{1, 2, \dots, m\}) \setminus \emptyset \right\}, \tag{1}$$

$$\underline{A} = \left\{ (\min_{i \in J} a_{ik})_{k=1}^n \mid J \in P(\{1, 2, \dots, m\}) \setminus \emptyset \right\}. \tag{2}$$

Based on definition (1) set  $\bar{A}$  with a natural arrangement  $\leq_{\bar{A}}$  gives the *upper semi-greed* with the highest element  $\max A$ , denoted by  $a^*$  and called *the best alternative*. Similarly, set  $\underline{A}$  with natural arrangement  $\leq_{\underline{A}}$  gives the *lower semi-greed* with the lowest element  $\min A$ , denoted by  $a_*$  and called *the worst alternative*. Now, in the set  $L = \bar{A} \cup \underline{A}$  a partial arrangement that keeps both  $\bar{A}$  and  $\underline{A}$  arrangements can be defined. Here, for all  $a, b \in L$ , if  $a \leq_{\bar{A}} b$  will be  $a \leq b$ , and if  $a \leq_{\underline{A}} b$  will be  $a \leq b$ . In the principle,  $(L, \leq)$  is a partially arranged set that can be considered as a sum of the upper and lower semi-greed. Let  $a, b \in L$ , where  $a < b$  or  $a$  is covered by  $b$ . Then, for each criterion  $c_k$ ,  $k \in \{1, 2, \dots, n\}$  the preferred alternative  $b$  over alternative  $a$  in relation to criterion  $c_k$  can be defined as follows (Žižović, et al., 2014):

$$\delta_k(a, b) = Z_k(a, b) \cdot \frac{b_k - a_k}{a_k^* - a_{*k}}. \tag{3}$$

Now, if  $a, b \in L$  are two arbitrary alternatives, and  $P: a = p_1 < p_2 < \dots < p_j = b$  is a path in  $L$  from alternative  $a$  to alternative  $b$ , then, the current preferred alternative  $b$  over alternative  $a$  in relation to the criterion  $c_k$ , alongside path  $P$ , if  $\delta_k(p_i, p_{i+1}) = 0$  for all  $i \in \{1, \dots, j\}$ , and  $\delta_k^P(a, b) = 0$  the other vice is defined as (Žižović, et al., 2014):

$$\delta_k^P(a, b) = \frac{1}{\sum_{i=1}^{j-1} Z_k(p_i, p_{i+1})} \sum_{i=1}^{j-1} \delta_k(p_i, p_{i+1}), \tag{4}$$

or its equivalent:

$$\delta_k^P(a, b) = \frac{1}{\sum_{i=1}^{j-1} Z_k(p_i, p_{i+1})} \sum_{i=1}^{j-1} Z_k(p_i, p_{i+1}) \frac{p_{k+1,i} - p_{ki}}{a_k^* - a_{*k}}. \tag{5}$$

Starting from alternative  $a$  to alternative  $b$ , the goal  $L$  can be reached in more different ways with corresponding current preferred alternatives. So, the preference for alternative  $b$  over  $a$  in relation to criterion  $c_k$  can be defined as follows (Žižović, et al., 2014):

$\pi_k(a, b) = \max \{ \delta_k^P(a, b) \mid P : a \rightarrow b \}$ , and therefore the preference of alternative  $b$  over  $a$  can be viewed as  $n$ -tuple:  $\pi(a, b) = (\pi_k(a, b))_{k=1}^n$ . Thus, the distance of alternative  $a \in L$  from the best alternative  $a^*$  is given by:

$$D_1(a) = \frac{1}{\sum_{k=1}^n z_k} \sum_{k=1}^n z_k \cdot \pi_k(a, a^*), \quad (6)$$

Similarly, the distance of the worst alternative  $a_*$  from the alternative  $a$  is given by:

$$D_0(a) = \frac{1}{\sum_{k=1}^n z_k} \sum_{k=1}^n z_k \cdot \pi_k(a_*, a). \quad (7)$$

Now, for the two alternatives  $a, b \in A$  it can be said that alternative  $a$  is preferred over alternative  $b$  if alternative  $a$  is closer to the best alternative and the worst alternative is further from alternative  $a$ . If both alternatives,  $a$  and  $b$ , have the same distance from the best and the worst alternatives, then the alternatives  $a$  and  $b$  are *indifferent* or they are *incomparable*.

The relations (6) and (7) are partially arranged. If decision makers want to have total arrangement the following relation can be constructed:

For all  $a \in A$ , a difference is defined as:

$$D(a) = D_0(a) - D_1(a). \quad (8)$$

Total arrangement can be defined for all  $a, b \in A$ , if and only if:

$$D(a) > D(b), \quad (9)$$

Where  $a$  is preferred over  $b$ , and

$$D(a) = D(b) \quad (10)$$

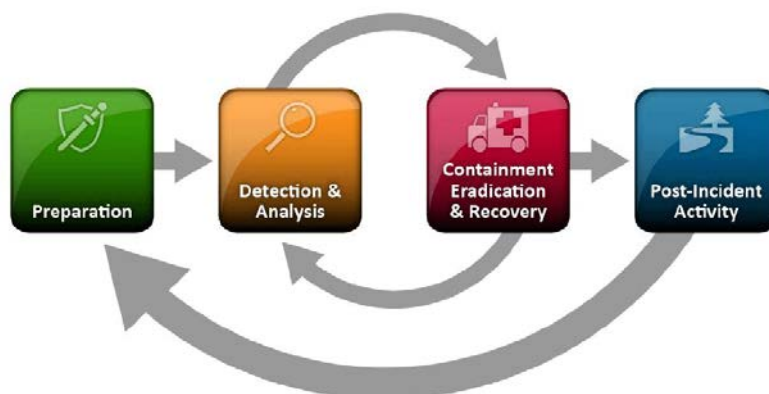
Where  $a$  is indifferent to  $b$ .

In this article, the *greed MCDM method* (Žižović, et al., 2014) is adopted and evaluated by the *Expert Choice* interactive software tool. *Choice of the optimal CCIDFI model in small and medium organizations* is set up as the goal of MCDA. Using *Expert Choice* interactive software tool integrated with greed MCDM method presents a novel approach to decision making process regarding digital forensic readiness in business environment.

The inability of the security mechanisms of the reactive and even proactive information security systems to discover and permanently prevent repetition of a sophisticated attack is the main reason for choosing an optimal CCIDFI model. The next step in the maturing



process of CI management is hiring an experienced DF investigator as a consultant. Integration of an expert with digital forensic knowledge, tools and skills into the security team is a mature CI management process (Kent, et al., 2006). As it is quite expensive for the average company, the choice of an optimal CCIDFI model seems to be a natural solution. A typical CI management model is shown in figure no. 1 (Cichonski, et al., 2013).



**Figure no. 1: Typical model of the CI management process**  
*Source: Cichonski et al., 2013*

In improving CCIDFI readiness some alternatives and their functional descriptions can be considered (table no. 1).

**Table no. 1: Functional description of the chosen CCIDFI alternatives**

$A_i$	Functional description of the CCIDFI alternatives
$A_1$	Command line forensic tool application by system/network administrator as first response to the computer incident/crime without use of DF science principles and procedures.
$A_2$	Provision of an open source or commercial DF tool for CCIDFI and application of DF principles and procedures by competent information security specialist, or hired DF consultant that provides authentic DD for potential DF analysis.
$A_3$	Provision of a tool for CCIDFI as in $A_2$ and application of DF science principles and procedures by a competent DF investigator that is integrated into the information security team providing authentic DD for potential DF analysis.
$A_4$	Combined alternative $A_3$ with a system of proactive DF of the computer network – strong monitoring and logging of forensically relevant data in all active network devices, for easier future DF investigation.
$A_5$	Proactive network forensic system integrated with central log server and DF tool as in alternatives $A_2$ and $A_3$ .
$A_6$	Ethical hacking and live forensic system integration into alternative $A_5$ for DF investigation of running web servers.

$A_1$	<b>Functional description of the CCIDFI alternatives</b>
$A_7$	Integrated $A_5$ and $A_6$ alternatives with predictive security mechanism – expert systems, data mining techniques etc. – for DF investigation and analysis of most sensitive computing systems such as Cloud Computing in real time.

Even though the order of the alternatives is not important for many MCDM methods, the authors, in table no. 1, suggest their ascending values starting from  $A_1$  to  $A_7$ . These alternatives can be evaluated using various criteria. Let us assume that we evaluate the seven CCIDFI alternatives using four main criteria, based on the *greed MCDA* method (Žižović, et al., 2014) and the *Expert Choice* tool. The criteria for evaluation of the alternatives can be chosen according to their importance and represented by the KPI or weight factors in the average company (table no. 2).

**Table no. 2: Chosen criteria and their normalized weight factors for each of the CCIDFI alternatives**

$C_k$	<b>The criteria for evaluation of the CCIDFI alternatives</b>	<b>KPI or weight factors <math>z_k \in (0,1]</math></b>
$C_1$	Cost of the CCIDFI process	0.9
$C_2$	Forensic image authenticity	1.0
$C_3$	Forensic investigator/analyst competency	0.7
$C_4$	Quality of the DE for admission in court	0.8

Source: Realized by authors based on Žižović et al., 2014.

Among all possible solutions of the CCIDFI alternatives, the one that performs well in all considered criteria should be the ideal choice. As there is unlikely to be a single best solution for all the considered criteria, a trade-off between the criteria is usually necessary. Functional descriptions of the criteria for the evaluation of each alternative are given in table no. 3.

**Table no. 3: Functional descriptions of the chosen criteria**

$C_k$	<b>Functional descriptions of the chosen criteria</b>
$C_1$	Cost increases using commercial DF tools, network forensics, the number of incompatible platforms and new devices with unknown architecture and hardware, and by the virtual environment Cost decreases using known file systems, familiar DF techniques and SOPs
$C_2$	To be admitted in court, the forensic acquisition and analysis must preserve the integrity of the DE in the custody chain
$C_3$	The competency of the DF investigator and analyst is relevant for DE admission by a judge

$C_k$	<b>Functional descriptions of the chosen criteria</b>
$C_4$	The quality of the DE, such as relevance, completeness, corroboration, harmfulness and coverage for the case, is required for legal admission of the DE

Suggestions for the preferred  $C_k$  weight factors for the optimal CCIDFI alternative evaluations are shown in table no. 4.

**Table no. 4: Suggested  $C_k$  weight factors for evaluation of the CCIDFI alternatives**

$A_i$	$C_k$ weighted factors			
	$C_1$	$C_2$	$C_3$	$C_4$
$A_1$	20	15	9	8
$A_2$	18	17	12	12
$A_3$	15	19	16	18
$A_4$	12	20	18	18
$A_5$	11	20	18	19
$A_6$	10	20	19	19
$A_7$	9	20	20	20

In this article, an assumption is made that all criteria are maximized and ranked from 1 to 20, where 20 is the best, and 1 is the worst weight factor. Certainly, it is possible to set up some other criteria for the CCIDFI alternative evaluations, but the authors of this paper considered that these criteria are appropriate for the CCIDFI optimal model choice in many practical cases.

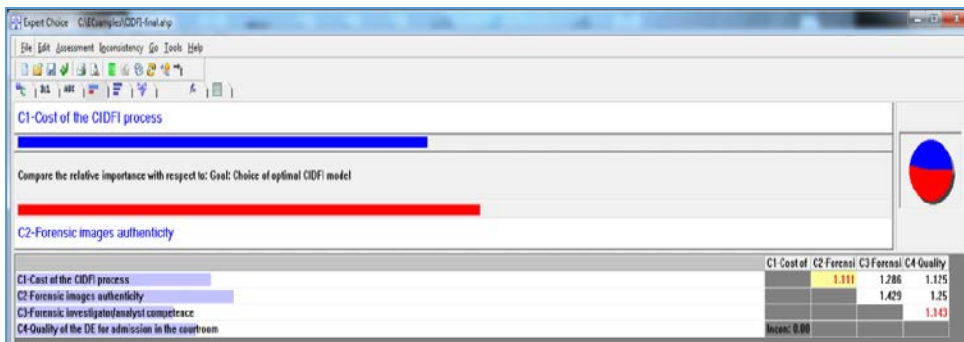
**3. Results and discussion**

Evaluation of the suggested alternatives, based on the *greed MCDM* method was undertaken by the multi-objective decision *Expert Choice* support tool, based on the mathematical Analytic Hierarchy Process (AHP) theory, first developed at the Wharton School of the University of Pennsylvania by one of *Expert Choice's* founders. The AHP helps decision making process by using both empirical data and the subjective judgment of the decision makers, providing them by a structure to evaluate the values of various criteria and the preferences of alternative solutions. Using what-if and sensitivity analyses, and pair wise comparisons to derive more accurately priorities than other MCDM methods, the *Expert Choice* combines these priorities for each solution to get the overall priorities of the alternatives and to determine how a change in the criterion value would affect choice of the alternatives (Barfod, 2014).

The choice of the preferred solutions among all the alternatives can be based on their relative value in *Distributive mode*, or on a single best alternative in *Ideal mode* of the *Expert Choice* tool.

In the *Distributive mode*, the normalized weight of criterion is distributed among all the alternatives. Then, all criteria weight is divided up into proportions that corresponds to the relative priorities of the alternatives. The *Ideal mode* maintains the rank of the best alternatives, unlike the *Distributive mode*. In it, the preferred alternatives are divided by the largest value among them and multiplied by the weight of the corresponding parent node. In that way, the most preferred alternative receives entire group priority given by the criterion immediately above it. The other alternatives receive a proportion of the parent node weight. The alternative that is best for all the criteria obtains value of one, while the other alternatives obtain proportionately less values. All the alternatives together give the sum more than one (Teknomo, 2006).

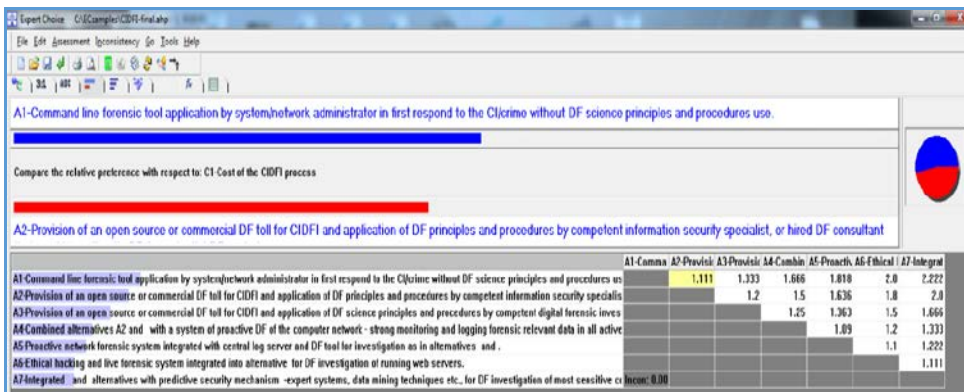
In the case study, the weight factors of the  $C_k$  criteria changed a few times to choose the optimal CCIDFI alternative or set. The comparative review of the relative impact among criteria  $C_k$  in the accomplishment of the main goal is shown in figure no. 2.



**Figure no. 2: Comparative review of relative impact among criteria**

Source: Authors calculations using Expert Choice Interactive Software tool

The set of optimal CCIDFI alternatives according to the established goal of this MCDM is shown in figure no. 3.



**Figure no. 3: Set of optimal CCIDFI alternatives**

Source: Authors calculations using Expert Choice Interactive Software tool

3.1 Evaluation of the results

To obtain the optimal solution set that could be acceptable for many companies of different sizes, an analysis of the *Expert Choice* results using both the *Ideal* and *Distributive modes* was undertaken. The same input parameters were used in both modes (figures no. 2 and no.3). The goal, criteria and CCIDFI alternatives that were evaluated in the *Ideal* mode are represented in figure no. 4.

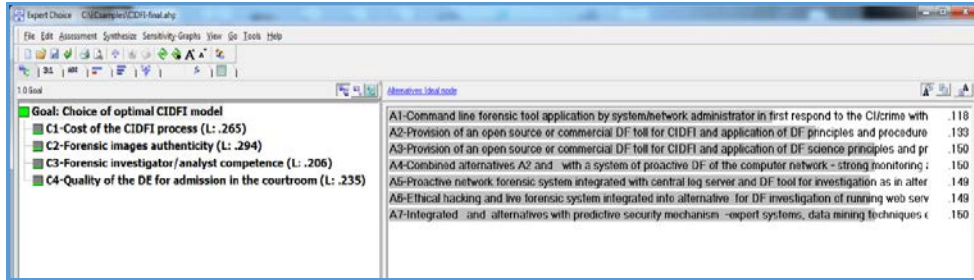


Figure no. 4: The goal, criteria and CCIDFI alternatives in *Ideal mode*  
 Source: Authors calculations using *Expert Choice Interactive Software tool*

The comparative values of criteria  $C_k$ , their influence and the results of the alternatives analysis, both given in percentages, are shown in figure no. 5.

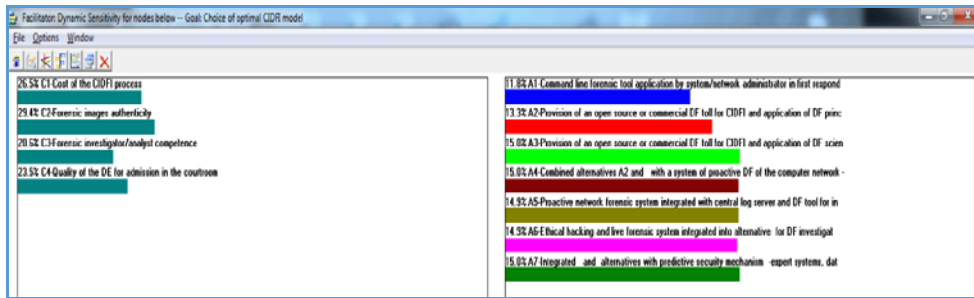


Figure no. 5: Comparative values of criteria  $C_k$ , their influence and results of alternatives' analysis  
 Source: Authors calculations using *Expert Choice Interactive Software tool*

In the *Ideal* mode, three alternatives,  $A_3$ ,  $A_4$  and  $A_7$ , have values of 15% and represent a set of optimal solutions. The values of the other alternatives are as follows  $A_5$  and  $A_6$  (14.9%),  $A_2$  (13.3%), and  $A_1$  (11.8%). Having a set of optimal alternatives, in addition, another three alternatives are analyzed to simplify the CCIDFI choice for the companies using only one or two criteria.

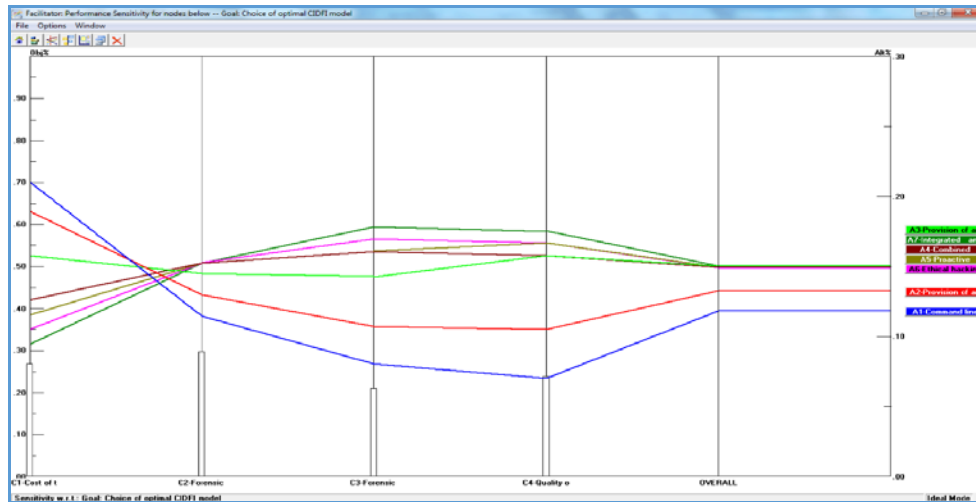
The summarized results of the "Head to Head" analysis by the *Expert Choice* software tool are given in table no. 5. The values all of the  $C_k$  criteria for each pair of alternatives are compared relating to each criterion.

**Table no. 5: Head to head analysis of the A<sub>3</sub>, A<sub>4</sub> and A<sub>7</sub> alternatives**

$C_k$	Weight head to head between alternatives $A_3, A_4$ and $A_7$	The best solution(s)
$C_1$	$A_3 > A_4; A_3 > A_7; A_4 > A_7;$	$A_3$
$C_2$	$A_3 < A_4; A_3 < A_7; A_4 = A_7;$	$A_4, A_7$
$C_3$	$A_3 < A_4; A_3 < A_7; A_4 < A_7;$	$A_7$
$C_4$	$A_3 = A_4; A_3 < A_7; A_4 < A_7;$	$A_7$

The results of the analysis confirmed that the  $A_3$  alternative becomes the optimal solution for the company choosing the  $C_1$  criterion as the most preferred. For companies choosing  $C_2$  as the preferred criterion, the set of alternatives,  $A_4$  and  $A_7$ , is the optimal solution. The authors suggested that alternative  $A_7$  should be chosen as it is most favorable from the forensic investigator and analyst point of view. The alternative  $A_7$  is the optimal solution for the choice of the  $C_3$  and  $C_4$  criteria.

Combining two or more criteria and obtaining the results, and the optimal solution using *Expert Choice*, analysis becomes a more complex process due to choice of the starting set for the optimal solution from three criteria by increasing  $C_k$ . The ‘performance sensitivity’ analysis in *Ideal mode* (figure no. 6) shows how the alternatives were prioritized relative to other alternatives with respect to each criterion as well as overall.



**Figure no. 6: The ‘performance sensitivity’ analysis in *Ideal mode***  
 Source: Authors calculations using *Expert Choice Interactive Software tool*

The goals, criteria and alternatives that were analyzed by the *Expert Choice* tool in *Distributive mode* are shown in figure no. 7.

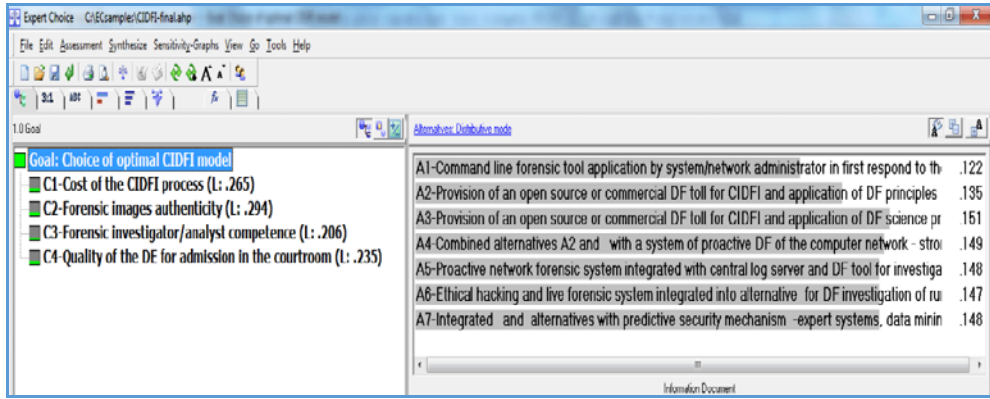


Figure no. 7: The goals, criteria and alternatives analysed in *Distributive mode*

Source: Authors calculations using Expert Choice Interactive Software tool

Compression of the criteria values, their impact on the alternatives and the results of the alternatives analysis (both in %) are given in figure no. 8.

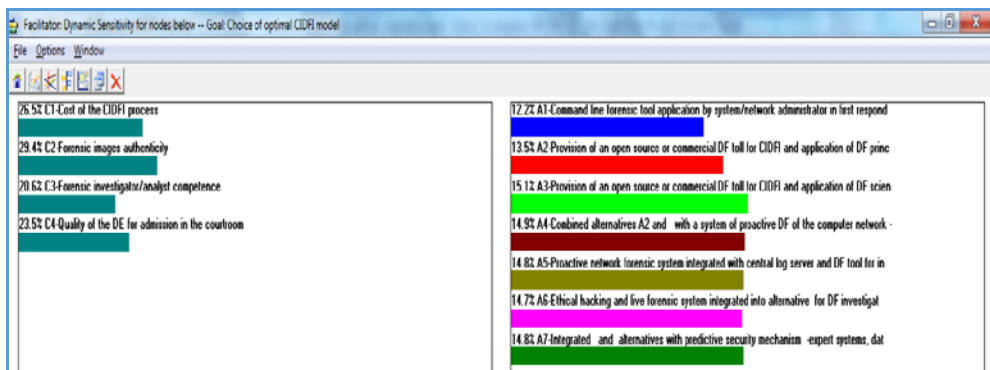
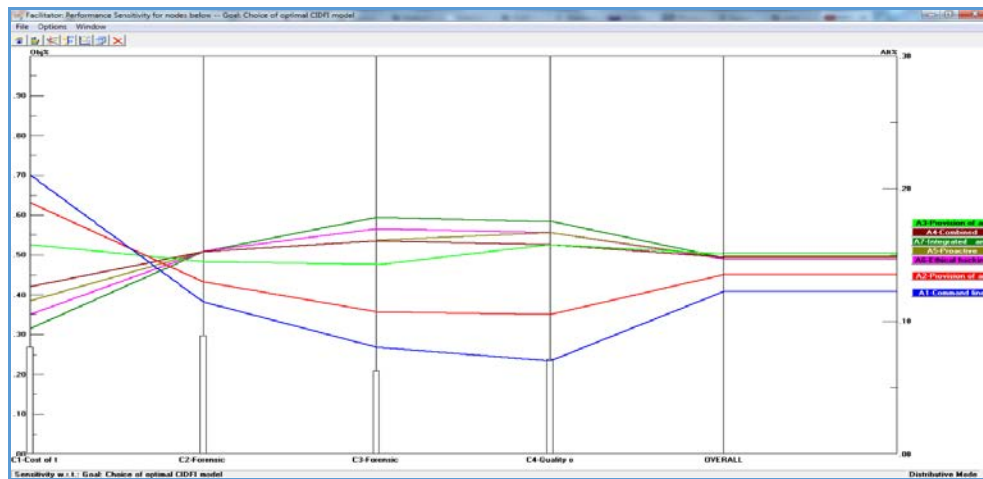


Figure no. 8: Compression of criteria values, their impact and results of analysis (in %)

Source: Authors calculations using Expert Choice Interactive Software tool

Analyzing the results of the evaluation in *Distributive mode* it can be seen that there is only one optimal solution,  $A_3$  (15.1%), and the other solutions of the CCIDFI alternatives are as follows:  $A_4$  (14.9%);  $A_5$  and  $A_7$  (14.8%);  $A_6$  (14.7%);  $A_2$  (13.5%), and  $A_1$  (12.2%). The ‘performance sensitivity’ analysis in *Distributive mode*, displayed in figure no. 9, shows how the alternatives were prioritized relative to other alternatives with respect to each criterion as well as overall.



**Figure no. 9: The ‘performance sensitivity’ analysis in Distributive mode**  
 Source: Authors calculations using Expert Choice Interactive Software tool

## Conclusions

In an environment of highly sophisticated threats and exploitation tools, and methods of attack, CI management becomes an inevitable part of a company’s management process. Due to the complexity of management phenomenon, the first response and the CI investigation require integration of the DF investigator into the information security team. In many private companies there is no appropriate capacity for CI management due to the lack of expensive technology and a competent DF investigator. That is why the choice of the optimal CCIDFI model becomes the most important activity in the CI management process. In this paper, use of the *greed* MCDM method in choosing the optimal model, combined with the *Expert Choice* software tool whose purpose is to evaluate an optimal set of the CCIDFI model alternatives is suggested by the authors as a new, integrated approach that aims to accomplish companies’ missions and sustain world-class results in order to become more competitive. The intention of given research was to help SMEs in managing their risk of fraud committed by using information technologies through optimization of forensic readiness of companies.

It is supposed that the CCIDFI alternatives should include similar DF investigation resources, principles, procedures and tools to those used by law enforcement, with the exception of arresting and sanctioning the attackers. As various companies have different capacities for CCIDFI, depending on size and CCIDFI readiness, the suggested approach in the choice of the optimal CCIDFI model alternatives or set can help companies to make better decisions. The main purpose of this work is to help company managers to validate their decision to employ a DF investigator and analyst as part of the information security team to improve the CI management process, increase forensic readiness and prevent possible future losses which, together with previously mentioned elements, have direct impact on company's business excellence.

In order to improve CCIDFI readiness, the authors considered seven crucial alternatives and four criteria for their evaluation. The ideal choice, among all possible solutions of the



CCIDFI alternatives, should be the one that performs well in all considered criteria. In the *Ideal* mode, three alternatives,  $A_3$  (provision of a tool for CCIDFI as in  $A_2$  and application of DF science principles and procedures by a competent DF investigator that is integrated into the information security team providing authentic DD for potential DF analysis),  $A_4$  (combined alternative  $A_3$  with a system of proactive DF of the computer network – strong monitoring and logging of forensically relevant data in all active network devices, for easier future DF investigation) and  $A_7$  (integrated  $A_5$  and  $A_6$  alternatives with predictive security mechanism – expert systems, data mining techniques etc. – for DF investigation and analysis of most sensitive computing systems such as Cloud Computing in real time), represent a set of optimal solutions.

The results of the analysis confirmed that Alternative 3, as the most preferred, becomes the optimal solution for the company choosing the first criterion – “Cost of the CCIDFI process”. For companies that chose “Forensic image authenticity” as the preferred criterion, the set of alternatives,  $A_4$  and  $A_7$ , is the optimal solution. Looking from the forensic investigator's and analyst's point of view, the authors suggested that Alternative 7 should be chosen as it is most favorable. As for the choice of “Forensic investigator/analyst competency” and “Quality of the DE for admission in court” criteria, the Alternative 7 is the optimal solution. Analyzing the results of the evaluation in *Distributive mode* it can be seen that Alternative 3 is the only optimal solution.

Experimental verification by the *Expert Choice* software tool, both in *Ideal* and *Distributive mode*, and evaluation of the results confirmed that an optimal CCIDFI alternative or set of them can be determined and can help small and medium-sized companies to strengthen their CCIDFI readiness and CI management processes in order to assess and manage risk and achieve or improve their business excellence.

## References

- Ab Rahman, N.H. and Choo, K.K.R., 2015. A survey of information security incident handling in the cloud. *Computers and Security*, 49, pp. 45-69.
- Alharbi, S., Moa, B., Weber-Jahnke, J. and Traore, I., 2012. High performance proactive digital forensics. *Journal of Physics: Conference Series*, 385(1), p. 012003.
- Anwar, T. and Abulaish, M., 2014. A social graph based text mining framework for chat log investigation. *Digital Investigation*, 11(4), pp. 349-362.
- Barfod, MB, 2014, *Graphical and technical options in Expert Choice for group decision making*. [pdf] Technical University of Denmark. Available at: <[http://orbit.dtu.dk/files/104238680/DTU\\_Transport\\_Compendum\\_Part\\_3\\_Group\\_decision\\_making\\_.pdf](http://orbit.dtu.dk/files/104238680/DTU_Transport_Compendum_Part_3_Group_decision_making_.pdf)> [Accessed 20 May 2016]
- Bradford, P. and Hu, N., 2005. A layered approach to insider threat detection and proactive forensics. In: s.n. *the Twenty-First Annual Computer Security Applications Conference (Technology Blitz)*. s.l., n.d. s.l: s.n.
- Casey, E., 2011. *Digital evidence and computer crime: Forensic science, computers, and the internet*. s.l: Academic press.

- Choo, K.K.R., 2011. The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 30(8), pp. 719-731.
- Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2013. Computer Security Incident Handling Guide. *International Journal of Computer Research*, 20(4), p. 459.
- Damodaran, A., 2007. *Strategic risk taking: a framework for risk management*. s.l: Pearson Prentice Hall.
- Dyck, I.J., Morse, A. and Zingales, L., 2013. How pervasive is corporate fraud?. *Rotman School of Management Working Paper*. (2222608)
- FireEye, 2013. *CISO Guide to Next Generation Threats: Combating Advanced Malware, Zero-Day and Targeted APT Attacks*. [online] Available at: <[http://www2.fireeye.com/rs/fireeye/images/fireeye\\_cisoguide\\_wp.pdf](http://www2.fireeye.com/rs/fireeye/images/fireeye_cisoguide_wp.pdf)> [Accessed 24 March 2016]
- Geoffrion, A.M., Dyer, J.S. and Feinberg, A., 1972. An interactive approach for multi-criterion optimization, with an application to the operation of an academic department. *Management science*, 19(4-part-1), pp. 357-368.
- Gibson, D., 2014. *Managing risk in information systems*. s.l: Jones and Bartlett Publishers.
- Giles, S., 2012. *Managing fraud risk: a practical guide for directors and managers*. s.l: John Wiley and Sons.
- Gorzalak, K., Grudziecki, T., Jacewicz, P., Jaroszewski, P., Juszczak, L., Kijewski, P. and Belasovs, A., 2011. Proactive Detection of Network Security Incidents. *ENISA report*.
- Greco, S., Figueira, J. and Ehrgott, M., 2005. Multiple criteria decision analysis. *Springer's International series*.
- Grubor, G. and Njeguš, A., 2012, November. Application of proactive digital forensics in Cloud Computing environment. In: s.n. *Telecommunications Forum (TELFOR)*. s.l, n.d. s.l: s.n.
- Haack, J.N., Fink, G.A., Maiden, W.M., McKinnon, A.D., Templeton, S.J. and Fulp, E.W., 2011, April. Ant-based cyber security. In: s.n. *Eighth International Conference on Information Technology: New Generations (ITNG)*. s.l, n.d. s.l: s.n.
- International Standards Office, 2013. ISO/IEC DIS 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements*. ISO
- Jones, K.J., Bejtlich, R. and Rose, C.W., 2005. *Real digital forensics: computer security and incident response*. s.l: Addison-Wesley Professional.
- Kaufman, J. R., 2012. *Intrusion Detection and Incident Response*. [online] Available at: <<http://faculty.business.utsa.edu/rkaufman/IDLsn4.ppt>> [Accessed 24 March 2012]
- Keeney, R.L. and Raiffa, H., 1993. *Decisions with multiple objectives: preferences and value trade-offs*. Cambridge: Cambridge university press.
- Kent, K., Chevalier, S., Grance, T. and Dang, H., 2006. *Guide to integrating forensic techniques into incident response*. [pdf] NIST Special Publication. Available at: <<http://cybersd.com/sec2/800-86Summary.pdf>> [Accessed 24 May 2016]
- Köksalan, M.M., Wallenius, J. and Zionts, S., 2011. *Multiple criteria decision making: from early history to the 21st century*. s.l: World Scientific.
- Köksalan, M.M. and Sagala, P.N., 1995. Interactive approaches for discrete alternative multiple criteria decision making with monotone utility functions. *Management Science*, 41(7), pp. 1158-1171.

- Martini, B. and Choo, K.K.R., 2014. Distributed filesystem forensics: XtremFS as a case study. *Digital Investigation*, 11(4), pp. 295-313.
- Nikkel, B.J., 2014. Fostering incident response and digital forensics research. *Digital Investigation*, 11(4), pp. 249-364.
- Salabun, W., 2015. The Characteristic Objects Method: A New Distance-based Approach to Multicriteria Decision-making Problems. *Journal of Multi-Criteria Decision Analysis*, 22(1-2), pp. 37-50.
- Scarfone, K. and Mell, P., 2007. *Guide to intrusion detection and prevention systems (IDPS)*. [pdf] NIST Special Publication. Available at: <[http://ecinetworks.com/wp-content/uploads/bsk-files-manager/86\\_SP800-94.pdf](http://ecinetworks.com/wp-content/uploads/bsk-files-manager/86_SP800-94.pdf)> [Accessed 22 February 2016]
- Steel, C., 2006. *Windows forensics: The field guide for conducting corporate computer investigations*. s.l: John Wiley & Sons.
- Team, C.P., 2010. *CMMI for Services, version 1.3*", [pdf] Pittsburg: Software Engineering Institute. Carnegie Mellon University. Available at: <<http://www.sei.cmu.edu/reports/10tr034.pdf>> [Accessed 22 November 2015]
- Teknomo, K., 2006. *Analytic hierarchy process (AHP) tutorial*. [pdf] Available at: <[http://www.thecourse.us/5/library/AHP/AHP\\_Tutorial.pdf](http://www.thecourse.us/5/library/AHP/AHP_Tutorial.pdf)> [Accessed 15 April 2016]
- Triantaphyllou, E., 2013. *Multi-criteria decision making methods: a comparative study*. s.l: Springer Science & Business Media.
- Uhl, A. and Gollenia, L.A., 2016. *Digital enterprise transformation: A business-driven approach to leveraging innovative IT*. s.l: Routledge.
- Vona, L.W., 2012. *Fraud risk assessment: Building a fraud audit program*. s.l: John Wiley & Sons.
- Weistroffer, H.R., Smith, C.H. and Narula, S.C., 2005. Multiple criteria decision support software. In: Anon, 2005. *Multiple criteria decision analysis: state of the art surveys*. New York : Springer, pp. 989-1009.
- Wu, D.D., Chen, S.H. and Olson, D.L., 2014. Business intelligence in risk management: Some recent progresses. *Information Sciences*, 256, pp. 1-7.
- Zimmerman, S., 2010. Proactive Computer Forensics. *Digital Forensics Magazine*, iss. 3.
- Žižović, M., Damljanović, N., Vićentijević, K., Kaljević, J. and Žižović, M., 2014. A multicriteria approach to the organization of work of computers in small and medium-sized enterprises from the perspective of protection and forensics. In: s.n. *XV International Scientific Conference "SINERGIJA2014"*. December 2014, Bijeljina, Bosnia and Herzegovina. Bijeljina: Sinergija University.