Corporate Digital Incident Investigation

DOI: 10.12776/QIP.V20I1.656

Jaromír Veber, Lea Nedomová, Petr Doucek

Received 16 December 2015, Revised 09 April 2016, Accepted 19 May 2016

ABSTRACT

Purpose: Information and communication technology are fundamental part of most business entities. Unfortunately, use of these technologies needs to be secured, and in the case that stipulated and legal regulations are not observed, it is very important to not only recognize but also prove such actions/incidents on time. Therefore, the ability to investigate the events/incidents in organization using traces in the information systems may be key component for regulation enforcement.

Methodology/Approach: We propose a model for digital investigations within the organization, based on ISO standards and existing models for common digital investigations.

Findings: The result of our work is a model that can serve as a guide to draft procedures for digital investigations within the organization. Such a procedure should provide evidence of a quality comparable to forensic evidence.

Research Limitation/implication: Our model provides an overview of the entire process and recommendations for its implementation; However, it does not provide a list of specific examination methods, because they vary depending on the case.

Originality/Value of paper: Most of the previously presented models for digital investigations were focused on the investigation of the police forensic laboratories. The originality of our model lies in its focus on investigations in the business organization.

Category: Conceptual paper

Keywords: digital investigation; business; organization; ISO; process; model.

1 INTRODUCTION

As information and communication technologies (ICT) keep developing and are being increasingly used in e-commerce, e-government, social networks and other areas, they more and more influence the regular life of citizens as well as the running of organizations regardless of their legal form. An information society (Webster, 1994) brings rapid information changes. This speed is a big challenge for those who - for some reason - need to keep reliable and provable information. These can be businessmen, officials, attorneys, judges or investigators.

This is an interdisciplinary issue since provability and reliability are terms associated with law, i.e. the legal sector, while safety and information are terms associated with the IT industry. This issue is the subject-matter of the discipline called forensic investigation.

Forensic investigation is a very fast growing branch that adjusts to all IT trends, in particular to everything related to data processing and storing and the means of communication. If we want to secure evidence in digital form, it is necessary to particularly observe the following principles (Ieong, 2006; ISO, 2011a):

Relevance – evidence must clearly correspond with the subject-matter of investigation and must be important for the investigation of an incident and there must be a good reason why evidence should be included in the investigation. Evidence must clearly confirm or disconfirm certain claims and may not allow more possibilities or interpretations.

Reliability – all processes used in analyzing potential digital evidence must be repeatable and auditable; evidence must be obtained in a provable, possibly repeatable and certainly documented or auditable way from reliable media (e.g. disks verified by their owner, the police or an expert in this field).

Sufficiency – qualified authorized persons (person), who conduct the initial securing of digital evidence, should take into consideration the size of an examined data sample in order to perform all activities necessary for requested findings; this includes information about the quantity of materials that they received for processing or, as the case may be, information about which material from which entity they requested and how this request was satisfied.

Digital evidence cannot be procured by just any person. It should be a person who is qualified and especially authorized to do so. Authorization means that such a person has the right to procure digital evidence, e.g. expert institutions or experts. In both cases, it is necessary to consider the qualifications of both institutions and experts. It is not possible e.g. to ask a constitutional law expert to secure digital evidence. Well, it is possible but if you submit such evidence e.g. in court proceedings, its value shall be a zero.

These principles represent the so-called Forensic Investigation Triangle, Fig. 1 (Ieong, 2006).

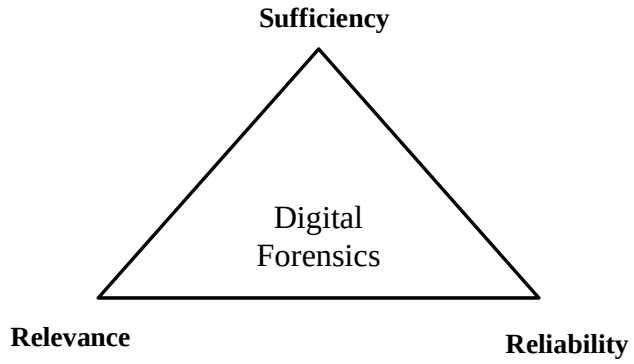

Figure 1 – Digital Forensic Investigation Fundamental, Source: (Ieong, 2006)

The actual principles of forensic investigation must be observed but for an investigation to be effective and purposeful, it is also necessary to take into consideration the processes and potential procedural models designed for forensic investigation. It especially concerns the famous Zachman model (Zachman, 2002). A simple model presented in (Carrier and Spafford, 2004) is shown in Fig. 2.

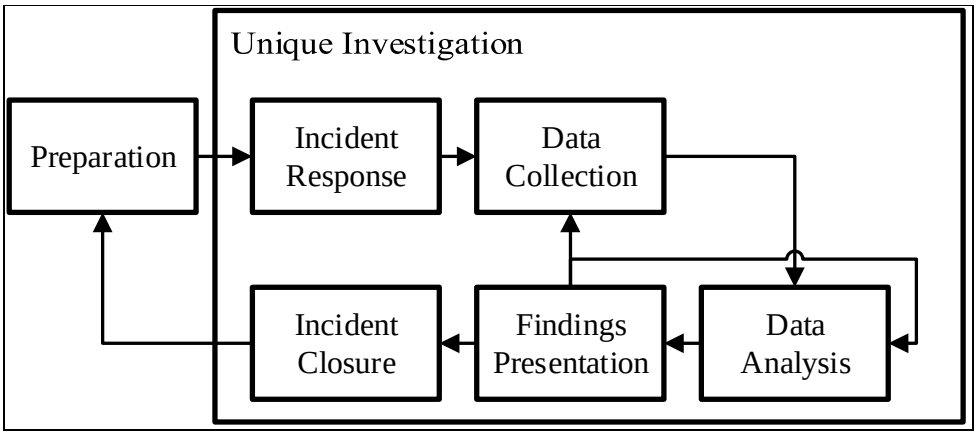

Figure 2 – Forensic Iteration Framework, Source: (Carrier and Spafford, 2004)

This model combines the procedures in securing digital evidence very well. It interrelates the preventive solutions of security incidents (Preparation), a response to an incident, data collection and follow-up data analysis. The analysis then provides data which must be interpreted and based on which the entire model of investigation may be modified.

The model (Carrier and Spafford, 2004) is then followed on with a procedural model of investigation on a higher level, which groups individual steps into phases. The advantage of the model is that it includes the phase of formulation of work hypotheses that are then verified. An example is provided in following Fig. 3.

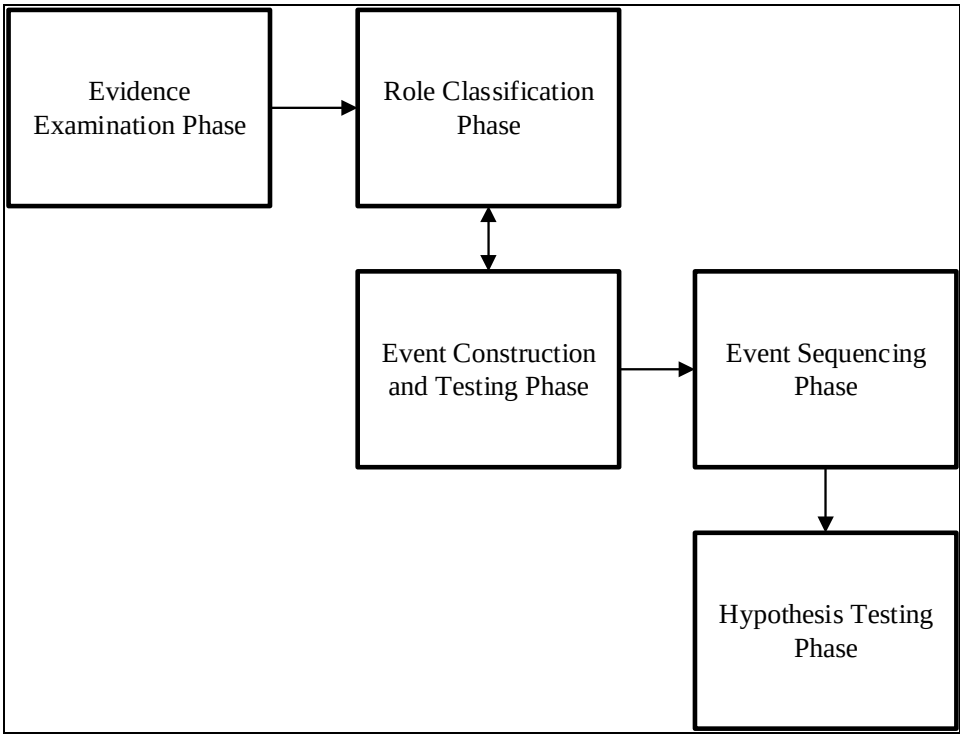

Figure 3 – Event Reconstruction Phases, Source: (Beebe and Clark, 2005)

The disadvantage of the model is that it does not include feedback allowing its permanent improvement and perfection, based e.g. on the ideas of the PDCA method. This is why the model is used more for *one-off application* rather than for *systematic investigation management*.

The area keeps developing and there are attempts for its standardization not only on the part of scientific workplaces (Beebe and Clark, 2005; Carrier and Spafford, 2004) but also on the part of ISO organizations. However, the majority of these publications mainly focuses on how **state authorities (the police)**, which most often conduct such investigations, should proceed.

2 STATEMENT OF PROBLEM

As the value and quantity of stored digital data keep growing, so does the risk that someone will try to make such data unavailable, to steal them or to tamper with them. For example surveys (Filkins, 2013; Villatte, 2015) present the most common threats to corporate security. A fairly large part of these incidents is currently illegal; however, their investigation and proving are usually not very successful. Moreover, there will always be incidents which are not punished by law yet disturb the running of an organization, and even these incidents must be

investigated and possibly punished. This concerns mainly misdeeds against in-house standards and regulations of a certain economic entity.

In this article, we focus on the procedures **in in-house investigations within an organization**. It concerns mainly misdeeds[1] that can be proven by forensic investigation. A thus defined area includes a relatively large number of misdeeds that may not be just of a "cybernetic" nature, but their traces are available in digital form and their consistent and correct analysis can provide necessary evidence proving such misdeeds. The investigation of different incidents can also be a part of an audit (Svatá, 2012).

We present general process (procedures) – that an organization should follow in order to obtain valid evidence from digital traces to prove incidents that violate the regulations of an organization. We also present how the process of digital investigation should be integrated into the organization.

We would like to point out that we will focus on the Czech Republic; however, our proposed recommendations should also apply to a large part of the European Union that already has a partly unified law as to working with information. We assume that the organizations, which are planning to implement our presented recommendations, already have an existing and functioning security management system, e.g. based on the recommendations of the family of standards ISO 27000. Furthermore, we would like to point out that our presented procedures are not designed for obtaining audiovisual evidence. To obtain audiovisual evidence, it may require using other procedures and techniques.

3 METHODOLOGY

Standardization in this area has been already tackled in (Hykš and Koliš, 2014; Veber and Klíma, 2014); however, the creation of a unified and comprehensive methodology requires more than that, it mostly requires a thorough analysis of the already existing models (Beebe and Clark, 2005; Bulbul, Yavuzcan and Ozel, 2013; Carrier and Spafford, 2004; Ieong, 2006; ISO, 2015a) together with the analysis of the law of the Czech Republic and the EU. In creating the model, we also included information received from experts who collect evidence in expert and police practice in the Czech Republic. Thanks to this, we were able to create a model that tries to take into consideration the recommendations from the models already presented in the past, including the model presented as part of ISO 27000. Our proposed model especially takes into account both the law of the Czech Republic and the specifics of investigation in an organization.

[1] This term is understood to mean any conduct that violates law or the in-house policies (regulations) of an organization.

4 RESULTS

In order to conduct a successful digital investigation, it is necessary to:

- detect/recognize an incident and,
- record sufficent data about the incident.

If an organization already have an incident management in place (Forte, 2007; ISO, 2011b; Mitropoulos, Patsos and Douligeris, 2006; Susanto, Almunawar and Tuan, 2011) it should be easy to detect and recognize an incident. If we do not recognize, or recognize late, such an event, we obviously cannot start a successful investigation.

The second necessity is to have *sufficient recorded data* about the event (incident). If we know that the incident occurred, but we do not have a sufficient quantity of recorded data about such an event, it will be difficult not only to identify the culprit but also to collect sufficient evidence to prove the investigated incident in order to achieve this goal it is necessary to focus a bit more on incident preparation phase.

Digital investigation process should be included as a process related to the incident management process. The conceptual incorporation of digital investigation in incident management is shown in Fig. 4.

Not until an incident (misdeed) is processed and sufficient information about the incident is collected can we start an actual investigation and use the methodology proposed by us. Of course, all this applies if it is necessary/appropriate to investigate the incident and to try to identify the culprit and to prove his misdeed.

However, before we start discussing the actual investigation, it is necessary to determine who will conduct the investigation, which depends on the seriousness of the misdeed. Let's divide misdeeds into three categories, depending on who is responsible for their investigation. Let's point out that the categories are mutually exclusive and therefore, if we are not sure, we should choose the category of a more serious misdeed. The categories are as follows:

- crime,
- civil dispute,
- violation of directives/policies of an organization.

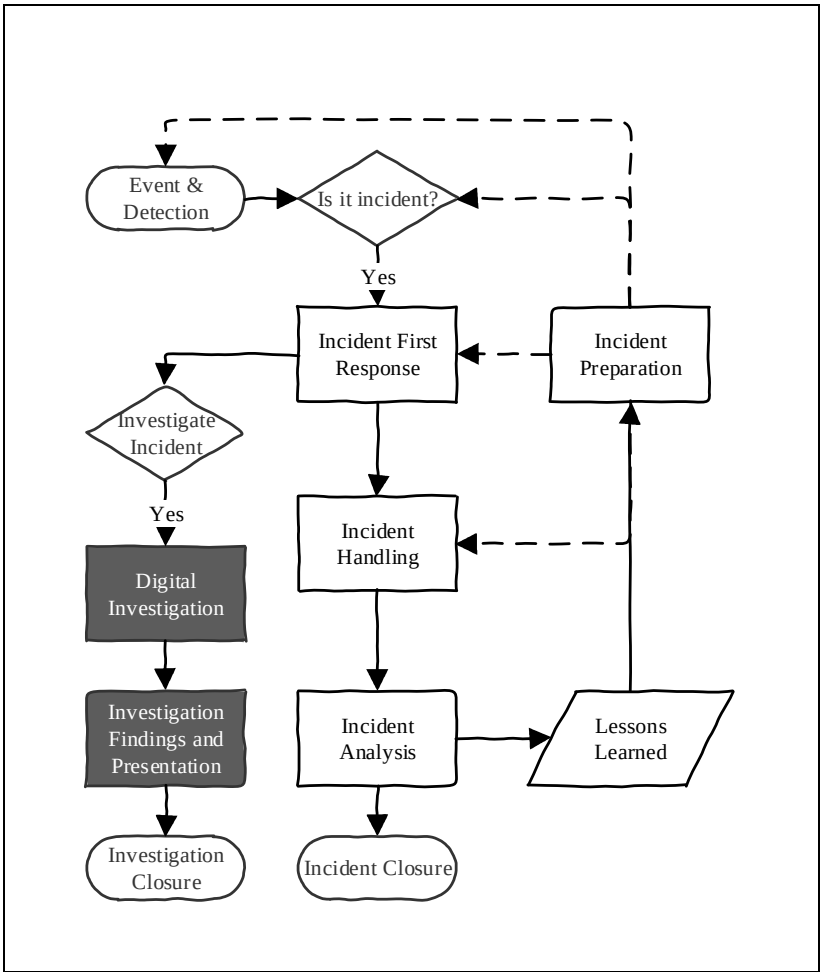

Figure – 4 Overall Event Handling Scheme, Source: (Authors)

The misdeeds, which fall under the crime category, are punished pursuant to the Penal Code and very often result in a considerable damage (over 5,000 CZK) or a grievous bodily injury. Evidence concerning a crime is collected by the police and the crime must be proven in court by the investigating authority. In such a case, an organization will only provide sufficient data and information to the police who will collect, process (analyze), store and interpret such data. Let's also mention that this kind of investigation is free of charge because police is funded by the state.

The misdeeds, which fall under the civil dispute category, are also resolved in court, but do not fall under the crime category (and for this reason they will not be investigated by the police). However, evidence used in court must be of legal value and for this reason, digital evidence must be prepared by a court expert. In such a case, if an organization wants to win the assumed civil dispute, it must hire a court expert experienced in digital investigation and provide him with

sufficient data/information for obtaining sufficient evidence. The hired court expert is then responsible for investigation.

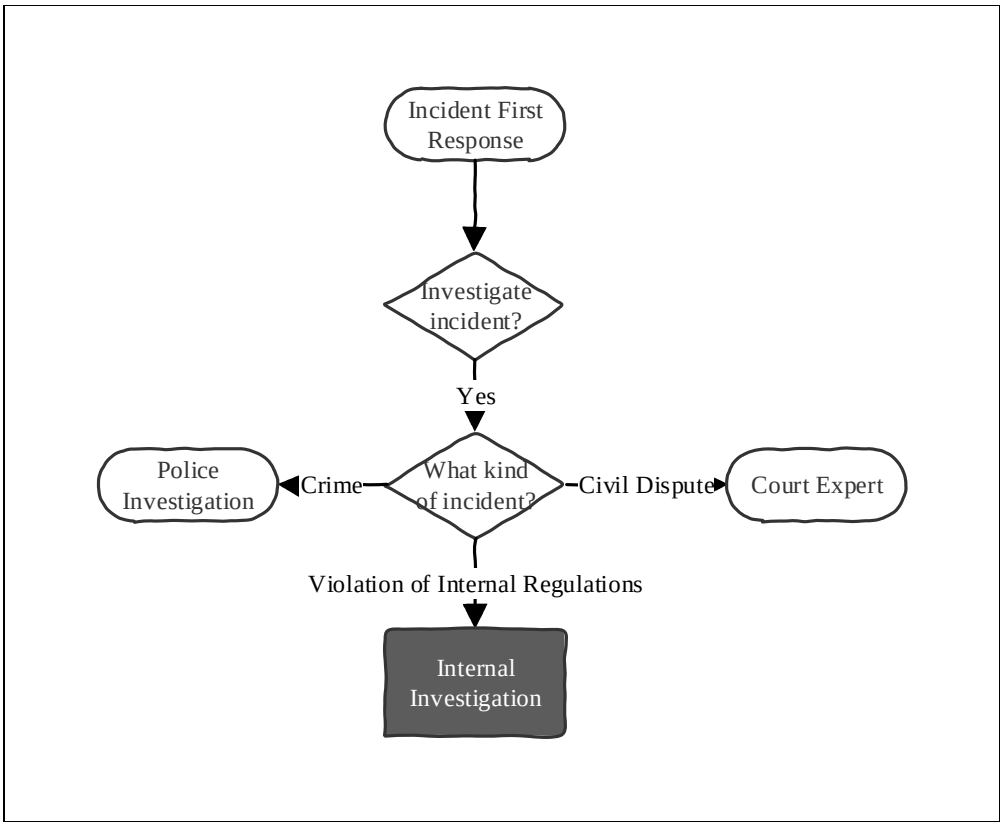

Figure 5 – Decision on the investigation procedure, Source: (Authors)

The last possibility is that a misdeed, which does not fall under any of the previous categories but violates directives/policies of an organization, and the organization management wishes to investigate it in order to find the culprit and prove his misdeed. In such a case, it is possible to use internal resources of the organization to investigate the entire matter. However, even in this case, an investigation should be conducted, using standard investigation methods. This is not only because it is necessary to prove the authenticity of obtained evidence to all parties involved, but also because there is a rather big risk that this misdeed will end up in court.

The initial investigation phase including incident detection and investigation decisions is demonstrated in Fig. 5.

In-house Investigation

Rules that cannot be neglected

An entire in-house investigation must be conducted in a very similar (same) way as the investigation of the police or a court expert. The main reason is the

provability and indisputability of obtained digital evidence for all parties involved, especially for the aggrieved party and the culprit. For this reason, the investigation process must observe the following requirements:

- Repeatability.
- Auditability.
- Justifiability.

Repeatability is understood to mean that an investigator, who obtained certain evidence, should be able to reach such evidence repeatedly, using documented procedures.

Auditability is understood to mean that the investigation procedures and results should be verifiable by any independent authorized party. For this reason, original data must always be available and must be recorded, and any procedure and method of data handling must be documented.

Justifiability is understood to mean that an investigator should be able to defend his actions and procedures. To defend is understood to mean to prove that the selected procedures and methods are the best way to obtain all possible pieces of evidence.

Personal Activities and Responsibilities

Digital investigation is strongly linked to incident management thus it is also possible that persons responsible for incident resolution may also do the digital investigation. In such case, the incident is resloved with regard to possible further investigation, and then followed by the actual search for digital evidence.

Despite sharing the responsibilities for incident management and investigation may suit smaller organizations it is certainly better to introduce two distuinguish groups of employees, where both are responsible for the incident preparation phase, but as soon as security incident occurs, one group is responsible for incident resution and the other for digital investigation, because it allows both processes to run simultaneously.

Overview of the entire investigation procedure

An investigation can be described as a sequence of consecutive steps, even though some steps can occur concurrently. First of all, let’s visualize the entire investigation as described in Fig. 6.

The initial phase has already been described above (Fig. 5). During this phase it is necessary to make several decisions, including the most important one, i.e. whether or not to investigate the problem/misdeed. Not until it is decided to investigate will the entire process of investigation start. During this phase, it must be also decided about who will conduct the investigation.

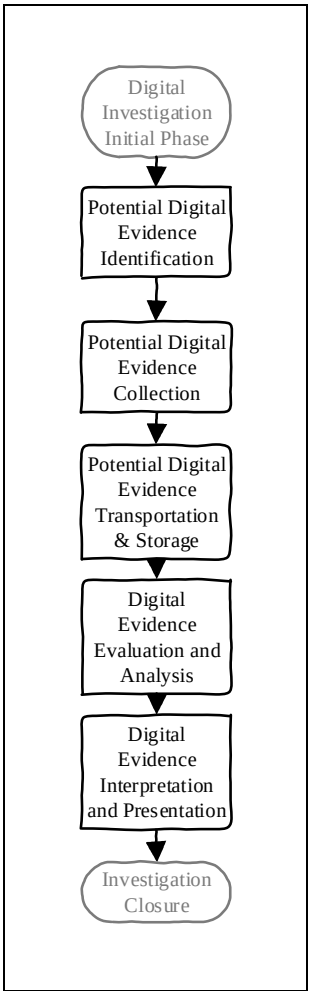

Figure 6 – Detailed investigation process, Source: (Authors)

During the **digital evidence identification** phase, it is necessary to arrive at the place where digital evidence will be collected. The place should be first documented (with photographs, if possible). After that it is necessary to find out what can contain digital evidence, i.e. what must be collected/acquired during investigation. Digital traces are most often found in devices that are able to store data in digital form. Such devices include all types of computers (PC, telephones, tablets,…), different portable data storage devices (flash disks, optical disks, self-contained hard disks,…) as well as other digital devices containing potentially important information (network elements, different built-in devices, …). Certain information related to the investigation can be hidden as a note on a piece of paper – these are often passwords, schemes or other information important for the investigation and for this reason, the entire investigated place should be thoroughly searched. If the investigation is conducted in an organization, it is very important that an investigator mainly focuses on whether or not a device

relates to the case – the publications (Leigland and Krings 2004; Beebe and Clark 2005) can be helpful here.

The phase of **collection of potential digital evidence** is illustrated in Fig. 7. During this phase, an investigator will evaluate whether or not it is possible to obtain digital traces from a device and how. In the case that an investigator secures data (binary image), he must right away also produce image hashes and document them. The entire data collection should be documented, i.e. which devices were identified in the previous phase, which devices were secured and from where, who secured them and how. During this phase, an ***impartial person*** should participate in the investigation and confirm by signing the secured digital traces report that the traces were secured in a standard way and that the obtained hash sums are authentic.

During the phase of **transport and storage of potential digital evidence**, an investigator must mostly make sure that potential digital evidence will not be modified or damaged, i.e. that nobody could tamper with them. He must also protect them from damage by different natural and other forces. During the transport phase as well, it is better that the secured devices (if any) be supervised (in addition to an investigator) by an impartial person. Secured data and data in secured devices should be kept for at least half a year after the case is closed.

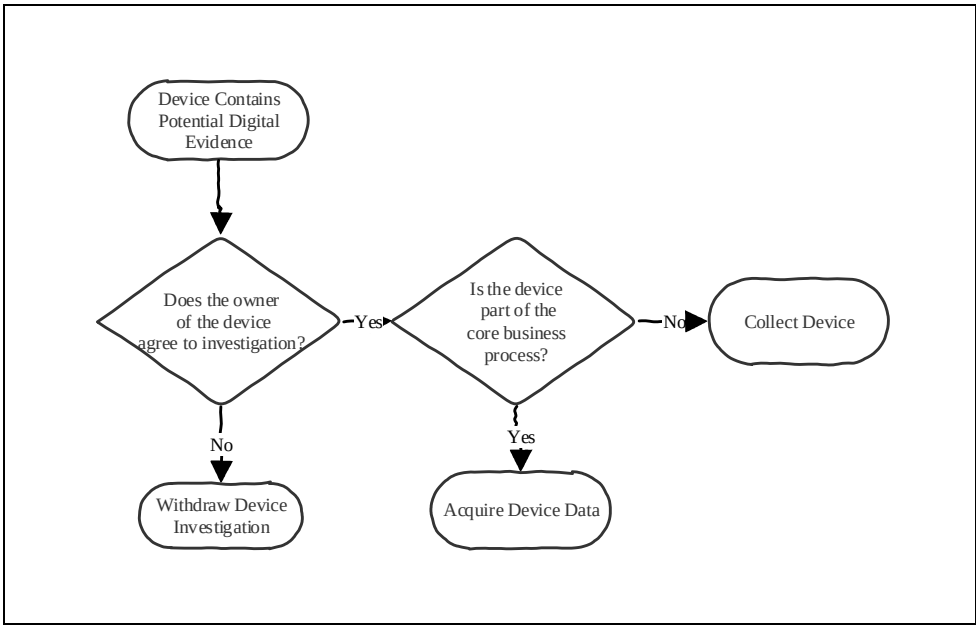

Figure 7 – Detailed potential digital evidence collection, Source: (Authors)

During the phase of **evaluation and analysis of potential digital evidence**, a search for evidence with respect to the given case is conducted. If devices were secured, the first task of an analyst is to obtain data (image) containing digital traces from such devices. Again, an impartial person should be present during this task and confirm (by signing the report) that the data were obtained from

secured devices and that hash sums above obtained data correspond. During this phase, it is possible to use different tools searching for strings or other information in the data. The tools that should be used are very well described e.g. in (Arasteh et al., 2007; Leigland and Krings, 2004; Srihari and Leedham, 2003); the use of valid methods is formalized e.g. in the international standard ISO/IEC 27042 (ISO, 2015b). An investigator should never work with original data, only with a copy or a copy of a copy, mainly so that the secured original data would not be damaged. Also, an investigator usually does not run any programs with secured data (except when programs are analysed, but even then, they must be run in an isolated environment – a sandbox).

During the phase of **interpretation and presentation of results**, the task of an investigator is to present the conclusions of his own investigation to third parties. An investigator must be able to clearly interpret and present investigation results to all parties involved. An investigator must be able to support his conclusions with obtained evidence and to prove that he obtained such evidence by means of his own documented procedures.

The closing of investigation is the last phase of investigation. The investigation reaches this phase when all parties agree with the conclusions and consequences of investigation.

5 COMPARISON TO EXISTING MODELS

Previous models (Beebe and Clark, 2005; Bulbul, Yavuzcan and Ozel, 2013; Carrier and Spafford, 2004; Ieong, 2006; ISO, 2015a) were focused on investigation itself - led by forensic experts or the police. We did not change the model for investigation itself, we think it is well developed; however, it is not that easy to fit it to business processes of the organization. We considered basic ideas of existing models for forensic investigation and we have added steps, needs and options of the environment within the organization. This means that our model should be easy to deploy in the organization.

We have also used charts based on business process notation making the process of digital investigation well understandable also for the top management of the organization. There is also a chart (Fig. 5) that should help with the most important decision (of the process) whether to start the internal investigation and who should be responsible for it.

Presented process model introduces the base for the *systematic investigation management* in the company led by its employees considering all the requirements of professional investigation.

6 CONCLUSIONS

This article presents a simple framework that can be used in investigating misdeeds in an organization after a security event or incident occurred. Using this presented framework should help organizations to implement digital investigation process. It is designated for public and state administration organizations as well as for the private sector. It is not designated for the investigating bodies of courts, experts or expert institutions. In view of the used legislation, the proposed procedure is primarily designated for organizations in the Czech Republic and is based on the conceptual chart shown in Fig. 6. The steps in the chart are progressively analyzed and their main activities are specified. The model is currently being tested in Czech practice in cooperation with the company RAC, s.r.o.

ACKNOWLEDGEMENTS

This paper describes the outcome of a research that has been accomplished as a part of research program funded by University of Economics, Prague IGA 74/2014 Innovation management system of digital forensics laboratories.

REFERENCES

Arasteh, A.R., Debbabi, M., Sakha, A. and Saleh, M., 2007. Analyzing multiple logs for forensic evidence. *Digital Investigation*, 4, September, pp.82–91.

Beebe, N.L. and Clark, J.G., 2005. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2), pp. 147–167.

Bulbul, H.I., Yavuzcan, H.G. and Ozel, M., 2013. Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Forensic science international*, 233(1-3), pp.244–256.

Carrier, B. and, Spafford, E.H., 2004. An event-based digital forensic investigation framework, In: *Proceedings of the 2004 digital forensic research workshop (DFRWS)*. Baltimore, Maryland , 11-13August, 2004.

Filkins, B., 2013. *The SANS 2013 Help Desk Security and Privacy Survey*. SANS Institute.

Forte, D., 2007. Security standardization in incident management: the ITIL approach. *Network Security*, 2007(1), pp.14–16.

Hykš, O. and Koliš, K., 2014. Development of the Digital Forensic Laboratory Management System Using ISO 9001 and ISO/IEC 17025. In. *IDIMT – Interdisciplinary Information Management Talks.* Linz: Trauner Verlag, pp.87-94.

Ieong, R.S., 2006. FORZA–Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3, September, pp.29–36.

ISO, 2011a. ISO/IEC 27005:2011, *Information technology – Security Techniques – Information security risk management.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2011b. ISO/IEC 27035:2011, *Information technology – Security techniques – Information security incident management.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2015a. ISO/IEC 27043:2015 *Information technology – Security techniques – Incident investigation principles and processes.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2015b. ISO/IEC 27042:2015 *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence.* International Organization for Standardization, Geneva, Switzerland.

Leigland, R. and Krings, A.W., 2004. A formalization of digital forensics. *International Journal of Digital Evidence*, 3(2), pp.1–32.

Mitropoulos, S., Patsos, D. and Douligeris, C., 2006. On Incident Handling and Response: A state-of-the-art approach. *Computers and Security*, 25(5), pp.351–370.

Srihari, S.N., Leedham, G., 2003. A survey of computer methods in forensic document examination, In: *Proceedings of the 11th Conference of the International Graphonomics Society (IGS2003)*, Scottsdale, Arizona, USA, 2-5 November 2003, pp.278–282.

Susanto, H., Almunawar, M.N. and Tuan, Y.C., 2011. Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences*, 11(05), pp.23–29.

Svatá, V., 2012. *Audit informačního systému.* Vyd. 2. Praha: Professional Publishing.

Veber, J. and Klíma, T., 2014. Influence of Standards ISO 27000 Family on Digital Evidence Analysis, In. *IDIMT – Interdisciplinary Information Management Talks.* Linz: Trauner Verlag, pp.103–114.

Villatte, N., 2015. *2015 Data Breach Investigations Report*. Verizon Enterprise Solutions.

Webster, F., 1994. What Information Society? *The Information Society*, 10(1), pp.1-23.

Zachman, J., 2002. The zachman framework for enterprise architecture. *Zachman International.*

ABOUT THE AUTHORS

Ing. **Jaromír Veber**, Ph.D. is the academic staff at the Department of System Analysis at University of Economics, Prague, Czech Republic. His main research and development work is specifically focused on the IS/ICT security management and cloud services, e-mail: jaromir.veber2@vse.cz

Mgr. **Lea Nedomová** has been working as assistant professor of the Department of System Analysis at the Faculty of Informatics and Statistics at the University of Economics, Prague, Czech Republic since 1996. Her main research and development topics include system approach to global society, sustainable development and its relation integrated management, e-mail: nedomova@vse.cz

Prof. **Petr Doucek**, Ph.D. heads the Department of System Analysis at University of Economics, Prague, Czech Republic. His main research and development work is focused on information management, IS/ICT security management, project management and impacts of information society on human and economy, e-mail:doucek@vse.cz