INFORMATION SECURITY CONTROLS AS DETERMINANT OF CONTINUITY OF INFORMATION SYSTEM WORK

Edin Osmanbegović[1], Nedžad Pirić[2], Mirza Suljić[3]

ABSTRACT

The purpose of this research is to identify the influence of information security controls on the continuity of information system work. The fact that the companies operate in highly turbulent business environment with severe threats to information security, leads to the need to examine this issue in detail. In their research, the authors have presented the indicators of impact of information security controls on the continuity of information system work. From the point of information security policy prescription, out of the total number of the surveyed companies, 80% do not have the required policy or a document showing the management commitment (attitude) to the introduction of information security measures. About 84% of the surveyed companies have information system access control. About 32% of these companies have the controls at the level of computer network, 22% of them have the control at the operating system level, while 38% have the control at the software application level. From the aspect of information system physical security, the surveyed companies (84%) indicated that they devote a considerable attention to this segment of information security. When analysing the existence of prescribed procedures for information system incident management, the study determined that only 20% of the companies have implemented these procedures. The prescribed procedures for monitoring information system continuity in the surveyed companies are at a very low level, as most of the companies (84%) do not have a proper procedure.

Keywords: information security, aspects and procedures of information security, information system continuity, protection of companies' information resources.

1. LITERATURE REVIEW

Despite a substantial number of studies conducted in the information security area, there is a lack of literature that connects the fields of information security and information system continuity which is the aim of this research. Information security policy represents a documents that defines the measures and standards of information security to be applied in the information system area to protect the confidentiality, integrity and availability of data and the availability and integrity of information systems in which the data is processed, stored or transmitted (Peltier, 2004). In a narrow sense, the information security policy document represents a statement of companies' top management underlining beliefs, goals, and reasons as well as the ways to reach the desired results in the field of information security, in the form of a short and concise document on a general level, with no specifics and detailed description (Klaić and Perešin, 2010). Information security policy aims at planning the requirements of information security, reaching a consensus in the company, making and implementing policy and reviewing the policy on a regular basis in order to meet safety requirements in the enterprise. Several theorists believe that information security can be achieved through establishment, implementation, and maintenance of information security policy. For example, Kabay pointed out that the establishment of information security policy should include five procedures (Kabay 1996):

1. Assess and convince the top management
2. Analyse the demands of information security
3. Form and develop policy
4. Implement policy
5. Maintain Policy

[1] *Faculty of Economics, University of Tuzla, Univerzitetska 8, 75000 Tuzla, BiH, edin.osmanbegovic@untz.ba*

[2] *Neutrino d.o.o., Klosterska 30, 75000 Tuzla, BiH, piric.nedzad@gmail.com*

[3] *ZD Rudnici „Kreka" d.o.o. – Tuzla, Mije Keroševića br.1, 75000 Tuzla, BiH, mirza.suljic@untz.ba*

Information security access control is considered as the most important aspect and pillar of information security. In a general and theoretical sense, information security access control is the provision of "freedom from risk and danger" (Umesh H. R., Umesha N., 2014). Information system access control relies on good practice which requires the establishment of the process management of hardware and software assets in all stages of their life cycle, including among other things, maintaining adequate inventory, naming the owner, i.e. responsible persons, defining the rules of acceptable use and safe disposal, etc. (Pantović et al., 2013).

Security controls regarding the access to the information system that are observed in this research are the controls at the computer network level, operating system level and at the level of users' applications.

The task of the access control at the network level is to prevent unauthorized network access and network services by implementing controls on internal and external networks through appropriate mechanisms to determine the authenticity of users and devices, as well as to implement control user access to information services (The ISO 27000 Directory, 2017).

Operating system access control aims to prevent unauthorized access to operating systems. In order to restrict access to the system authorized users, information security resources are used. An important aspect of access control operating systems is a software security, which mainly deals with operating system security, application security and security software tools, including security tools used to provide information security.

Access control at the application level is related to various business application controls, implementation control of information activities and operations (whether the transaction is accurate and complete, distribution of duties and control, authorization, etc.) and information services control (availability and functionality of the network infrastructure, data, equipment, etc.).

Physical security refers to the measures taken to protect the information system physical environment and infrastructure resources, including hardware, software and other networked devices against physical threats such as theft, fire, water, flood, and so on. The term information system physical security refers to the measures and methods of physical protection of the information system facilities and building infrastructure and environment to support the information and communication technology (ICT) from accidental or deliberate threats. Physical security is still an important part of any information system security and cannot be ignored, since it represents an important "line of defence" for most of the companies. This research addressed the following aspects of information system physical security (Umesh H. R., Umesha N., 2014):

- Basic physical protection in terms of obstacles such as fences, walls, doors, authentication devices, etc.
- Physical checks of entering such as access right to certain areas within the company
- Equipment safety in terms of the prevention of theft, loss or equipment damage, etc.
- Equipment placement and protection including placement and use in accordance with manufacturer's instructions
- Installation safety relating to prevention of damage to installations - Network Information System)

Information security incident management in the theoretical sense argues the view that the information security management is a part of unforeseen event management intended for prevention, detection and response to threats, vulnerabilities and impact inside and outside the company. This approach to unforeseen events is recognized and answers situational variables in order to effectively achieve the organizational goals. Information security incident management represents a timely and effective response to unplanned and unwanted events that may impair the safety or information system functionality.

Information system continuity is considered in the context of information security policy, physical security and information security access control and information security incident management. These measures, which were investigated in this research, should ensure smooth and continuous operation of all significant systems and business processes, as well as limit losses in emergency situations. This area is wider than the field of information systems management, but due to the fact that a small number of business processes in companies could be carried out without the availability of information systems, it is clear that the provision of information system continuity is crucial in business continuity planning and disaster recovery (Herbane et al., 2004).

ISO 27001: 2013 is information security standard, which is the specification for the Information Security Management System (ISMS).

The official title of the standard is "Information technology — Security techniques — Information security management systems — Requirements". ISO / IEC 27001: 2013 comprises ten short clauses and annexes.

ISO / IEC 27001: 2013 group controls addressed in this research are:

- **Information security policies** (2 controls) – this group controls how the policy is written and reviewed
- **Access control** (14 controls) - access control policy, managing user access, system and application access control and user accountability.
- **Physical and environmental security** (15 controls) - this group includes safe area definition, access control, threat protection, safety equipment, safe disposal, the policy of "clear the table and the screen", etc.
- **Information security incident management** (7 controls) - controls for reporting events and weaknesses, defining responsibilities, procedures for response to incidents and collecting evidence.
- **Information security aspects of business continuity management** (4 controls) - controls require business continuity planning, procedures, verification and inspection and IT redundancy (The ISO 27000 Directory, 2017)

Information system continuity represents an integral part of business continuity management (BCM), which in practice represents the set of processes and resources required to identify potential threats, calculate their potential impact and provide necessary practices for prevention, mitigation and recovery from the disturbance. Incidents of information technology and information systems affect business operations, because as shown in numerous examples, they can have a serious impact on the business. Businesses recognize the continuity of the information system as a key issue for information management. Information security enables keeping continuity of work of the information system, reducing the potential for damage, providing a return on investment (ROI) and improving overall operations.

2. METHODOLOGY OF EMPIRICAL RESEARCH

In the context of the primary research (field research), the data is collected using the method of testing, with a questionnaire as a technical means of data collection. The respondents were businesses and the members of management or persons responsible for implementation of information security in the enterprise.

The basic set of respondents includes organizations from the register of the Federal Statistics Office in Bosnia and Herzegovina (BiH), based on a stratified sample of 50 companies. The survey was conducted by personal interview, telephone or questionnaire delivered to businesses via the Internet (e-mail). Data collection was conducted in the period from December 2015 to January 2016.

While elaborating on the theoretical and methodological origin of the assessed problems and specific application considerations, deductive method was used, as well as the analysis and synthesis method, classification method, etc. The collected data was analysed using a Statistical Package for the Social Science (SPSS) 19.0 for Windows. The developed analysis was presented descriptively, in tables and graphs, and was interpreted against the hypothesis in order to make conclusions and check the achievement of the overall objective.

2.1. Research variables

The variables observed in the context of the empirical research are:

The independent variable relates to information security. Information security is the state of confidentiality, integrity and availability of data, which is achieved by applying the prescribed measures and standards, and organizational support for planning, implementation, verification and improvement of measures and standards.

The dependent variable is related to the information system continuity. Providing information system continuity refers to the business impact of information security incidents and formulates the ways in which the organizations can prevent them.

Indicators of independent variables represent the aspects of information security:

- Security policy
- Access Control
- Physical Security
- Information security incident management

The indicators of dependent variables are:

- Percentages of the companies that have prescribed and applied procedures of the information system continuity.

2.2. Analysis and discussion of the empirical research results

During the primary research into implementation of the information security measures in enterprises, the basic sample of 422 companies was used. By random sampling, 100 companies were selected and contacted, 50 of which responded to the questionnaire. Data collection started in November 2015 and ended in late December 2015.

During the data collection for the study, the limitations occurred when during the interviews an attempt was made to obtain the exact number of information security incidents, the length of information security incidents, the time needed for recovery and the potential impact of disruption to business operations. One company stated that it had no insight into the measure because the company headquarter was located outside BiH. At the same time, one of the companies believes that those parameters are confidential data that cannot be released for the purpose of the research. A representative of one surveyed company stated that he needed to seek additional management approval, while a representative of another company was on a field trip and was unable to provide an answer.

The questionnaire comprised 6 questions with sub-questions. The questionnaire was filled out by circling only one of the answers: Yes or No, and if the answer required so, the response was needed to sub-questions with Yes or No answers and further elaboration. If it was impossible to give a sufficiently precise answer this way, an additional comment was allowed in every response in order to fully describe the attitude of the company. The comment was not mandatory and the length of the comment was not limited. More than half of the respondents (52%) were interviewed by telephone, 26% were contacted through a field (personal) interview, while a minor share (22%) responded by e-mail.

2.3. Impact analysis of the information security measures

Based on the results of the primary research, it is evident that all the surveyed companies use information and communication technology (ICT) in their daily work and activities. In order to present a transparent and clear analysis based on the research results, the authors developed two models of information security. The theoretical model of information security represents maximum information security according to the aspects covered in empirical surveys (Models of authors of this paper). Information system maximum security is the level of information system security where all the studied information security aspects are at the highest (maximum 100%) possible level.

The actual or real security model presents the results of the empirical research, and as such represents the real level of the aspects covered by the empirical researches expressed in percentages.

Information security policy represents the essential document in information security implementation, which enables companies to plan, develop and implement a framework for managing information security, information assets, including financial information, intellectu-

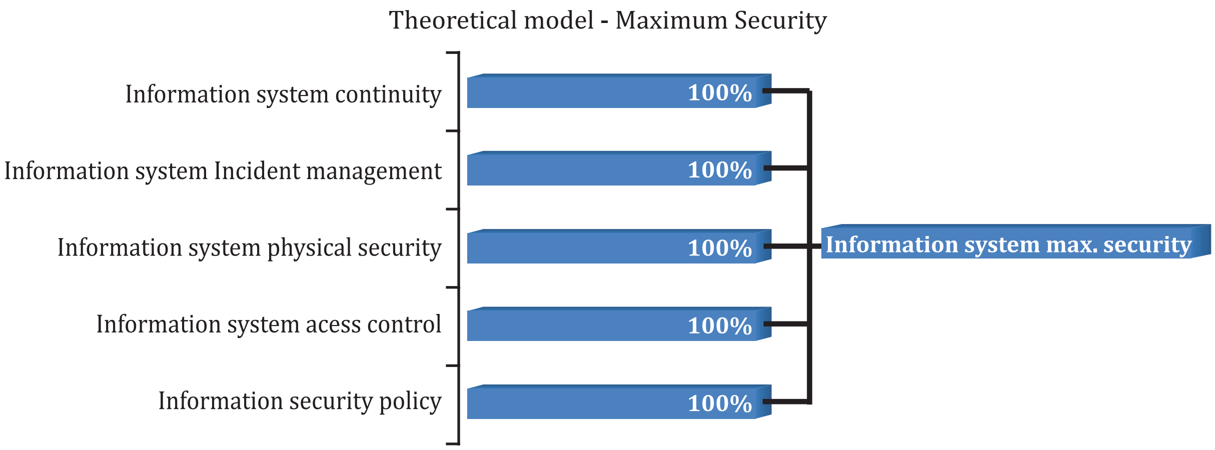

Figure 1. Theoretical model of information system maximum security

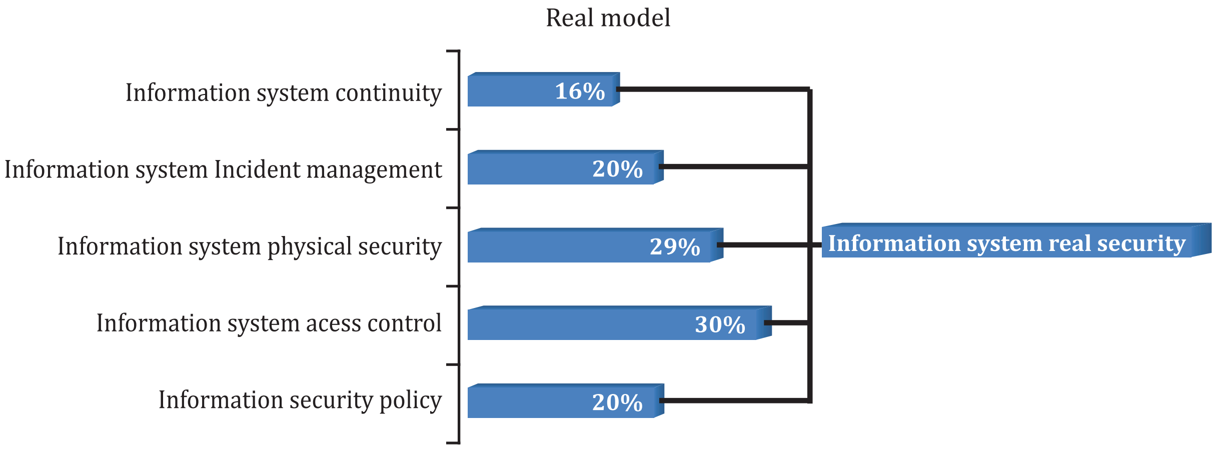

Figure 2. Actual (real) information system security model

al property, or entrusted information about the customer or the third parties. Out of the total number of the surveyed companies, 80% do not have the required information security policy which is an important indicator of the state of information security.

One of the positive survey results is in the segment of the information system access control availability in the surveyed enterprises at computer network level, operating system level and software applications level. The general indicator is that 84% of the companies have one, two or all three access controls. According to the presented results, the arithmetic mean indicates that the presence of access control in enterprises is 30%.

The research results related to the existence of information system physical security procedures represent another positive example of the security information system. The most of the companies (84%) have the prescribed procedures of information system physical security. All five of the controls mentioned in the survey are present in almost half of the surveyed companies (48%). The fact that 14% of the companies have no control of information system physical security represents a significant threat to the listed company's information system, because the procedure of information system physical security is the basis of information security. The average value of representation of the procedures for information system physical access is 28.66%, which is rounded to 29% for the purpose of an easier further analysis.

The research data analysis related to the existence of the prescribed procedures of information system incident management shows that 80% of the surveyed companies do not have the prescribed procedure for information system incident management, while internal controls for information system incident management is available in 14% of the companies. While observing the representation of standardized procedures for information system incident management, one enterprise (2%) uses the ISO 27001: 2013 certificate for information system incident management, as well as ISO 27001 certification and the GSMA, which totals 6%.

The existence of prescribed procedures for monitoring the continuity of information system work has the lowest representation in the overall study has, where as much as 84% of companies do not have the proper procedure, while 10% of the companies have internal procedures. As in the analysis of the previous aspects, 6% of the companies with standardized approach to information security are also the only companies with the proper procedures for monitoring the continuity of information system work.

According to the survey, information security in the surveyed companies is at a very low level. In most surveyed companies (72%) there are no written formalized information security procedures, which are the main assumption for considering information security as whole. Out of 28% of the companies confirming in the study to have formalized information security procedures, only 6% are certified / have the information security standards. What functions as an indicator of the state of information security and therefore the continuity of the information system, is the research data showing that more than half of the surveyed companies (56%) have absolutely no procedures for information security. In addition, out of the entire sample only one company (2%) has information security based on ISO / IEC 27001: 2013.

3. DISCUSSION OF THE EMPIRICAL RESEARCH RESULTS

Looking at the research results from the enterprise size aspect, 14% of the surveyed companies are large companies with over 250 employees, while 28% are medium-sized companies with 50 to 250 employees. The largest number (58%) is small enterprises with less than 50 employees. Over half of these companies (52%) are in trade (28%) and manufacturing (24%) business, which is over half of the sample.

Looking at the surveyed companies from the perspective of the establishment, 22% have been present on the market for over 20 years, while 24% of the companies exist between 15 and 20 years. Twenty-two percent of the companies have been present on the market between 10 to 15 years, while 20% were incorporated in the period of 5 to 10 years. Twelve percent of the analysed companies were established less than 5 years ago.

During the research, it was found that 24% of the surveyed companies are using IT outsourcing for information system management, which is a significant shift in use of IT services to specialized “third parties”. According to international practices, the use of IT outsourcing brings new threats and vulnerabilities to business performance, safety and continuity arising from growing interdependence on providers of the third-party service. Therefore, it is necessary to ensure that delegating activities do not jeopardise the safety or functionality of information system, that the company’s data remain in its possession, and that entrusting the activities should not whatsoever be an obstacle to smooth control in that part of business.

The presented research results explicitly show that the formalization of information security written procedures in the surveyed companies is at a very low level. The fact that there are only 6% of the companies that have a standardized approach to information security and that over half of the companies (54%) do not have any information security procedures clearly shows the lack of awareness and the lack of understanding of information security importance.

From the aspect of information security policy prescription, 80% of the total number of the enterprises do not have the required policy or document showing the management commitment (attitude) to the information security measures introduction. The survey showed that 14% of the companies have internal information security policies while

4% adopted the information security policy, and only 2% of the companies implemented information security policy according to ISO 27001: 2013. It is interesting to note that 8% of the surveyed companies are in the process of information security policy-making, which certainly is an encouraging step forward in terms of awareness of the importance of implementing the information security policy.

Eighty-four percent of the surveyed companies have information system access control, which is also an important positive indicator in information security management. Thirty-two percent of the companies have the control at the level of computer network, 22% have the control at the operating system level, while 38% have the control at the level of software applications. Cumulatively, 50% of the companies have all three controls. Eighteen percent of the companies have two controls and 22% of the companies have one control, while 10% of the companies do not have any information system controls.

From the aspect of information system physical security, the surveyed companies mainly stated (84%) that they devote considerable attention to this segment of information security. "The weakest link" (56%) in this context is the checking of entrances, i.e. the right of access to the premises of a company that has the components of the information system. The companies pay a lot of attention (84%) in terms of the barriers that protect the information system and take care of security equipment to prevent theft, loss or equipment damage (82%). Excellent results were achieved by (84%) the surveyed companies in implementation of equipment accommodation and protection in accordance with manufacturer's instructions. Seventy-six percent of the companies implemented security measures for prevention of damage to installations and network information system and for installation safety. By summarising the phenomenon of the prescribed procedures for information system physical security, it can be concluded that 58% of the companies have all five controls. Twenty-eight percent of the companies have four controls, while 10% of the companies have three controls. Fourteen percent of the companies have no control for information system physical access.

Analysing the availability of the prescribed procedures for information system incident management, the study found that only 20% of the companies have implemented the procedures. The same percentage of organizations (20%) has a prescribed procedure in accordance with the standard or internal procedure for information system incident management. From the aspect of the procedures representation for information system incident management, 2% of the companies use ISO 27001 certificate for information system incident management, one company has ISO 27001: 2013 certificate and one company GSMA certificate. Fourteen percent of the companies have internal controls for information system incident management. As stated above, 80% of the surveyed companies do not have the prescribed procedure for information system incident management.

Prescribed procedures for monitoring information system continuity in the surveyed companies are very low, so that most of the companies (84%) do not have proper procedure. From all the surveyed companies with prescribed procedures for monitoring information systems continuity (16%), the number of information system incidents (disruption) has been measured in 12% of the companies. As in the previous research question, a total information system outage time (disruption) has been identified and measured in 12% of the companies. The number of information system incidents that affect information system failure (disruption) has been measured in 16% of the companies, which is more than for the two previous measurements of information system continuity. As in the previous survey question analysis, three companies (6%) have information security standard procedures for monitoring the continuity of the information system.

4. CONCLUDING REMARKS

The results of the primary research have shown that only 20% of the surveyed companies have the prescribed information security policy, which is one of the most important indicators of the current state of information security in Bosnia and Herzegovina.

The empirical research has shown that information system access control is present in 30% of the surveyed companies, and it can be concluded that information system access control is underrepresented, which significantly threatens information system continuity.

The primary research results showed that information system physical access procedures are implemented in about 29% of the companies. Therefore, it may be concluded that insufficient implementation of measures securing physical access to information system directly exposes to risk the level of information security and information system continuity.

According to the presented survey results, 72% of the companies do not have or have only partially updated written information security procedures. This leads to a conclusion that due to the lack of or inadequately established information security written procedures, the surveyed companies lack the appropriate level of information security and are not able to provide adequate information system continuity.

Although the world trends show that the frequency of information security incidents is still on the increase, the conducted research shows that only 20% of the surveyed companies manage information security incidents properly, which leads to the conclusion that the lack of prescribed procedures for information security incidents management has a direct adverse impact on the information system continuity.

For future research, it would be suitable to study compatibility of operational, strategic and financial goals of enterprises in terms of information security. It is also needed to research the application of good practices in management of information assets along different phases of the information security life cycle. The mentioned research, if conducted, would give a much better insight in the resources needed to properly manage information security in enterprises.

5. REFERENCES

1. Džafić, Z., Osmanbegović, E., (2011), Entrepreneurship and Inovation: Case of Bosnia and Herzegovina, Proceedings of the 3nd International Conference: Management, izobraževanje in turizem, družbena odgovornost za trajnostni razvoj, 21. i 22 october, Portorož, Slovenia
2. Herbane, B., Elliott, D. & Swartz, E. M. 2004. Business continuity management: time for a strategic role? Long Range Planning, 37, 435-457.
3. Kabay, M. E. 1996. NCSA Guide to Enterprise Security, McGraw-Hill Companies.
4. Klaić, A. & Perešin, A. 2010. The concept of information security regulative framework. International studies, Zagreb.
5. Pantović, V., Petrović, S. & Ristić, R. 2013. MINIMUM STANDARDS OF INFORMATION SYSTEM MANAGEMENT IN FINANCE INSTITUTION. Banking Magazine.
6. Peltier, T. R., Information Security Policies and Procedures, Auerbach Publications, 2004
7. The Iso 27000 Directory. 2017. An Introduction To ISO 27001 (ISO27001) [Online]. The ISO 27000 Directory. Available: http://www.27000.org/iso-27001.htm [Accessed 01/09/2017].
8. Umesh H. R., Umesha N., The InfoSec Handbook, 2014, ISBN 978-1-4302-6382-1