The Impact of Information System Risk Management on the Frequency and Intensity of Security Incidents

Original Scientific Paper

Hrvoje Očevčić
Addiko Bank d.d.
Slavonska avenija 6, Zagreb, Croatia
hrvoje.ocevcic@gmail.com

Krešimir Nenadić
Josip Juraj Strossmayer University of Osijek,
Faculty of Electrical Engineering, Computer Science and Information Technology Osijek
Kneza Trpimira 2B, Osijek, Croatia
kresimir.nenadic@ferit.hr

Krešimir Šolić
Josip Juraj Strossmayer University of Osijek,
Faculty of Medicine
Cara Hadrijana 10/E, Osijek, Croatia
kresimir.solic@mefos.hr

Tomislav Keser
Josip Juraj Strossmayer University of Osijek,
Faculty of Electrical Engineering, Computer Science and Information Technology Osijek
Kneza Trpimira 2B, Osijek, Croatia
tomislav.keser@ferit.hr

Abstract *– The survey identified positive effects of work on information security risk management. Regarding the survey results of information system incidents, a significant reduction was recorded in the number of system downtime incidents. The scope of implementation of the risk assessment methodology is the whole ICT system, and therefore the implementation covers all parts of information assets. Positive effects are obtained by reducing the risk by known mitigation methods. Technical details of the implemented control measures were not considered in this paper. In accordance with the standards used in methodology development, significant and increasing levels of user awareness of ICT systems have been considered. The effects of all implemented measures have resulted in a significant increase in the availability of parts of ICT systems.*

Keywords *– downtime, risk assessment, risk mitigation, security incidents*

1. INTRODUCTION

Risk management is a process that involves identification, assessment, and prioritization of risks. A process or a method is a collection of related, structured activities or tasks that produce a specific service or a product. In case of risk management, the term process is related to management, and thus it implies all business and organizational activities in the act of coordinating the efforts of people or technology to accomplish the desired goals and objectives using available resources efficiently and effectively. This article discusses the processes associated with information or similar systems.

Once risks have been identified, they must then be assessed as to their potential severity of impact (negative impact, such as damage or loss) and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure, in the case of the probability of the occurrence of an unlikely event.

With proper information system risk management it is possible to reduce the frequency and intensity of risk-related incidents in the system [1]. The incidents include adverse events that have already happened in the operational part of the information system and the

information assets. It is easier to notice system weaknesses with risk management, but also to predict a possible adverse harmful event by using Bayes algorithm [2] and the calculation of posterior probabilities. The posterior probability indicates the likelihood of possible future events and it is calculated based on the estimated probabilities used in the risk assessment. [3], [4].

Section 2 describes the information system risk management methodology. This section shows information asset categories and its description of performance rating. Section 3 explains the environment used to conduct an experiment. Section 4 compares the frequency and intensity of security incidents and presents results. The next section gives a brief insight into future research. The conclusion is given at the end of the paper.

2. INFORMATION SYSTEM RISK MANAGEMENT METHODOLOGY

The methodology underlying the results of research presented in this paper includes resources classified into information assets. Information assets include seven categories of resources (as shown in Table 1):

Table 1. Categories of information assets

Category number	Information asset
1	Environment and infrastructure
2	Personnel
3	Hardware
4	Applications and their databases
5	Communications
6	Documents and data
7	Other

Resource categories are introduced to better facilitate a visibility risk assessment procedure. Categorization is not necessary to achieve results, but in the later analysis it provides a detailed statistical analysis. Each identified resource needs to be evaluated. Resource information assets are evaluated by assessing the impact according to the violation of information asset properties (Table 2). Information asset properties refer to confidentiality, integrity and availability. Properties are selected such that performance evaluation is applicable to all resource categories.

After having evaluated the impact, a risk assessment is conducted for information asset resources for the property where the effects of loss of properties are above the acceptable level. For each information asset resource it is necessary to select possible combinations of threats and vulnerabilities that together form information system risks [5].

Risk is a function of the probability that a threat will exploit an existing vulnerability, and cause loss of an information asset property. A threat and vulnerability evaluation presents the estimated probability of realization as a function of the actual technical characteristics of the environment and implemented security measures.

Table 2. Description of information asset performance rating

Rating	Description
No value or negligible	Assessed aspect (confidentiality, integrity, availability, etc.) is not relevant or does not exist; loss of CIAO is negligible; the resource can be easily replaced
Low value	Resources in which loss of confidentiality, integrity or availability indicates no significant impact on cash flow, legal and contractual obligations, or the reputation of the organization; resources where maintenance costs are negligible point to low costs of modifications
Mean value	Resources in which loss of confidentiality, integrity or availability could imply additional internal costs and a potential impact on cash flow, legal and contractual obligations or the reputation of the organization; resources where maintenance costs are low and can be exchanged for higher mean costs
High value	Resources in which loss of confidentiality, integrity or availability indicates the immediate impact on cash flow of the organization, the ability of a business, the reputation, or legal and contractual obligations; precious resources
Very high value	Resources in which loss of confidentiality, integrity or availability can cause a collapse of the organization, tremendous damage, the current business deadlock or a serious loss of public reputation.

The information system risk management process is a continuous repetition of identification, assessment and risk prioritization (Fig. 1) [1].

Following specific priorities for particular risks, the measures for diminishing risks to the level of acceptability or complete removal are determined. Measures to reduce risks are divided according to the implementation of security measures, transfer of risks to a third party, avoidance, and risk acceptance [8, 9]. By selecting some of the options for diminishing risks, the vulnerability grade is reduced, i.e. the probability that the recorded threat will exploit the vulnerability [6]. Threat assessment reduction is possible by transferring risks to a third party, or by avoiding risks, but only in special cases. If the risk cannot be reduced by the methods mentioned, risk acceptance is selected as a method for emphasizing the existing weaknesses [10]. Accepted risks are continuously monitored and observed, and they are involved in the process of threat and vulnerability re-estimation.

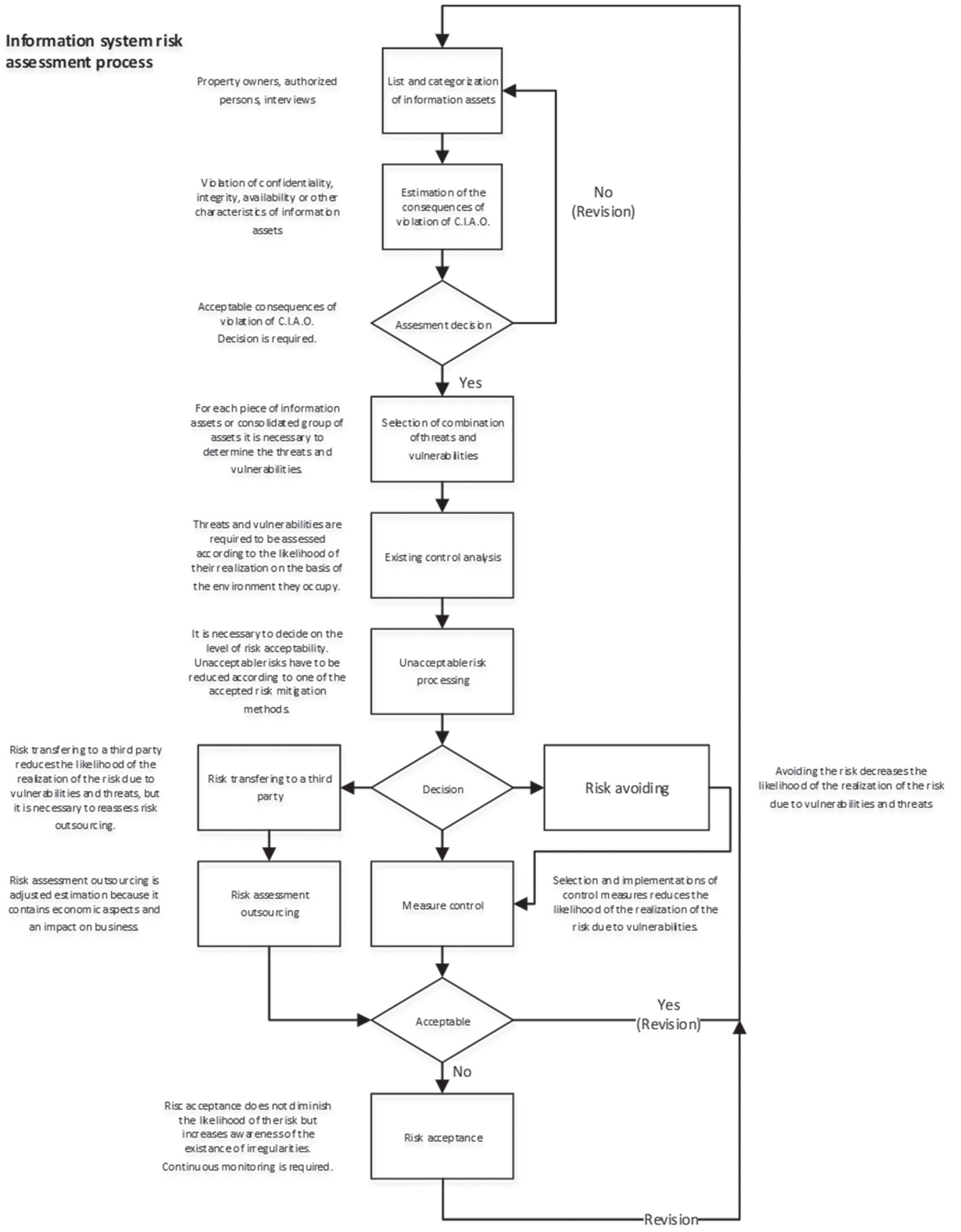

Fig. 1. Information system risk management process

3. RESEARCH AREA DESCRIPTION

Research area is an ICT system within the company, with no prior risk management during the period of time in which security incidents of the ICT system were registered. The information (ICT) system consists of 1,950 personal and laptop computers, 53 servers and 3 server rooms. The number of employees amounts to 1,700. Computer equipment is divided into personal computers, servers and virtual servers on VMware platforms. Operating systems are Windows, AIX and Linux. Databases are Microsoft SQL, Informix, Oracle and db2. Outsourcing of the parts of the information system has been contracted with external companies in relation to

business activities of development and software maintenance, as well as computer equipment parts.

After the implementation of the risk management methodology, information system security incidents were recorded [7]. Registration after the implementation of the risk assessment methodology was conducted in the same manner, and the criteria for incident evaluation and classification have not been changed. Periods in which the comparison has been carried out are the same and they are divided into quarters of the year. Within each quarter, a total number of incidents was analyzed according to the criteria of the records.

The contribution of this paper is based on measurements of the number of incidents over time during which implementation of the risk management methodology has been conducted.

4. COMPARISON OF THE FREQUENCY AND INTENSITY OF SECURITY INCIDENTS

This section presents an incident occurrence analysis, as well as definitions of measures that describe the intensity of the security incident. The research result lies in a significantly reduced number of security incidents (Fig. 2) in the field of information systems, in all aspects of frequency measuring, and the intensity of incidents.

The intensity is determined based on three components. The first component is the duration of the incident in the information system, and it is presented in the form of system downtime duration (Fig. 3).

The overall strength or intensity is determined on the basis of classified templates of potential incidents. The third component is the priority of the incident determined by the person responsible for the management of incidents and/or the affected system (Fig. 4).

Information systems can be divided into two groups, i.e. key systems and supporting systems. Priorities can be assigned according to the systems belonging to one of the mentioned groups. Key systems are those with loss of some of the properties of confidentiality, integrity or availability, assessed as critical for the organization, having a possibility to cause unacceptable losses.

In the period after the implementation of information system risk management, risks have been documented as follows:

- 262 risks recorded (potential risks and information system vulnerability);
- 93 unacceptable risks;
- 81 risks reduced to the acceptable level:
  - 59 by the implementation of security measures;
  - 10 by avoiding risks;
  - 8 by transferring to a third party;
  - 4 risks are accepted.

The incidents were recorded in the same way in the whole period of time and there is no difference in the criteria according to which the incidents are graded. The total number of recorded incidents fell by 50% in the same period of time. The most interesting information for business owners is the availability time of a business system. The percentage of availability is calculated in the same period of time and it is displayed in hours. Figure 5 shows the difference in hours for a period of recording incidents before risk management (99.97048%) and after implementation of the methodology (99.98684%). The difference is 85.97 hours for the entire testing period (3.5 days).

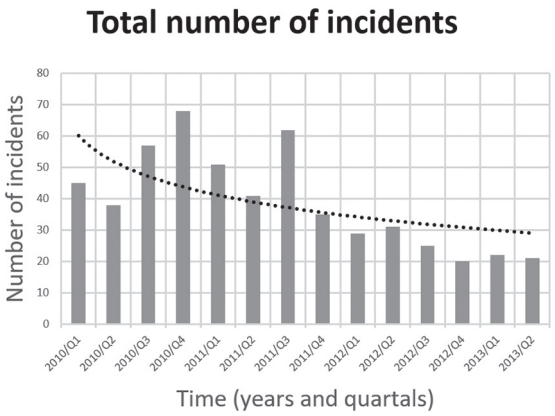

Fig. 2. Total number of incidents

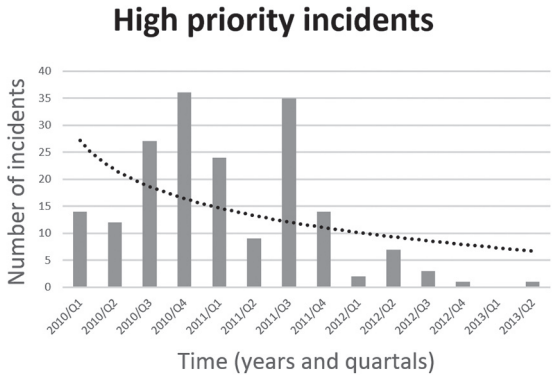

Fig. 3. Downtime duration

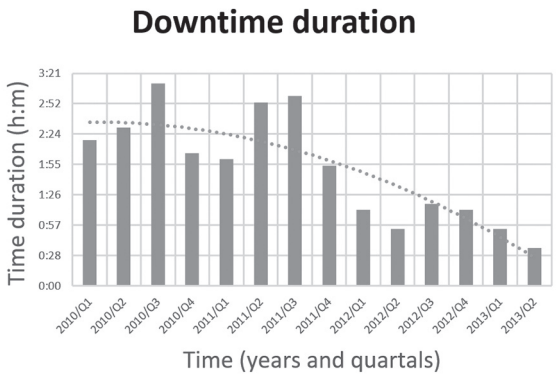

Fig. 4. High priority incidents

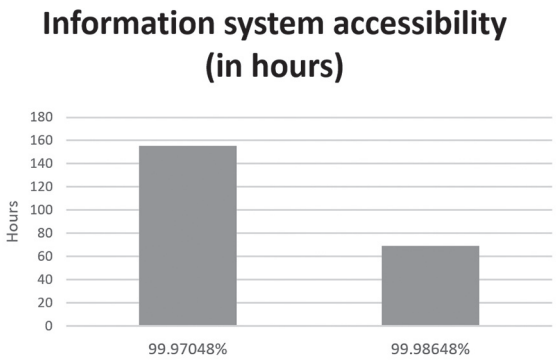

Fig. 5. Information system accessibility

Implementing the framework for information and communication technology risk management is in most cases carried out with the aim of reducing the number of adverse events and increasing the effectiveness and efficiency [13]. In addition to the benefits that risk management can bring to the personnel using information and communication technologies, it is useful to consider the economic impact [14], which is often the most interesting information in the decision-making process. Information system risk management raises the level of awareness among staff, but also creates an environment that systematically solves the problems associated with weaknesses and threats. The results of this research directly point to the benefits gained after the implementation of systematic risk management. Indicators such as downtime duration and the availability time directly point to the desired benefits of management.

5. FUTURE WORK AND RESEARCH

The impact of risk management outsourcing is an area regulated by a separate methodology, having a distinct tool developed for this purpose [6]. It is necessary to normalize measurement results of both risk assessment methodologies in order to make them comparable with each other. One of the possible measures to minimize risk is to transfer risk to a third party. Risk management externalization is a process that can consolidate risks within the company as well as those that have been transferred to a third party [10]. The process of externalization is often associated with strictly defined contracts and it is not possible to conduct supervision and risk management by third parties, but it can be expected that the implementation of the risk management externalization process can reduce security incidents that have occurred through externalization.

Risks recorded in the category "*Personnel*" are associated with the information system user habits, and during information system risk management such risks were reduced. By using ontology databases and algorithms capable of detecting risky user behavior, it is possible to reduce adverse effects of such events [5]. A combination of ontologies and calculation of the posterior probability with some algorithms allows us to define priorities based on the probability of adverse events. By using algorithms to calculate the posterior probabilities of adverse events based on estimation of the probability of threat realization and vulnerability from risk analysis, certain scenarios simulations can be created [12]. Risk situation scenario simulations provide a detailed insight into the environment and all associated parameters important for the preservation of the information asset properties [11]. There is some ongoing research in the area of decision-making support combined with Bayesian learning which is applied on an information system risk assessment. Questionnaires have been developed, providing an insight into user awareness of the information security process [15], [16], [17].

6. CONCLUSION

Information system risk management is a process that ensures a high level of awareness of personnel responsible for information system management. The initial implementation of risk assessment is a process that is more demanding administratively because it is necessary to implement the recording of assets and analyze the processes involved in the evaluation. Every subsequent assessment update complements the risk management process which highlights the vulnerabilities and threats, as well as the result of their influence, in addition to the recorded weaknesses. It is very important to define measures that objectively show the value of subjective analysis and values that are difficult to measure. Therefore, information asset properties are introduced in the process of estimation in the form of confidentiality, integrity and availability. Loss of any of the properties objectively represents a certain measure of the intensity of the incident. Measures of vulnerability and threats are presented as a probability of realization of these events and they depend on both the technical environment of information assets and the security measures implemented within that environment. Criteria for incident classification did not change during the time period the survey was conducted in. Also, the key parts of the information system did not significantly change either, except for minor changes. Minor changes to the information system are considered to be an acceptable fluctuation of staff and equipment within regular maintenance.

The largest advantage of the risk management methodology for company owners and management personnel is a significantly reduced information system availability time (3.5 days). On the other hand, for professionals working in ICT, a reduction in critical incidents and a significantly higher level of awareness in ICT systems is the largest advantage.

7. REFERENCES:

[1] D. J. Landoll, "The Security Risk Assessment Handbook", Auerbach Publications, 2006.

[2] C. P. Robert, "The Bayesian Choice, From Decision-Theoretic Foundations to Computational Implementation", Springer, 2007.

[3] X. Yang, H. Luo, C. Fan, M. Chen, S. Zhou, "Analysis of risk evaluation techniques on information system security", Journal of Computer Applications, Vol. 28, No. 8, 2008, pp. 1920-1924.

[4] I. Androutsopoulos, J. Koutsias, K. V. Chandrinos, G. Paliouras, C. D. Spyropoulos, "An Evaluation of Naive Bayesian Anti-Spam Filtering", Proceedings of the 11th European Conference on Machine Learning, Barcelona, Spain, 31 May 2000, pp. 9-17.

[5] C. Ghaoui, "Encyclopedia of Human Computer Interaction", Liverpool John Mores University, UK, 2006.

[6] R. Bojanc, B. Jerman-Blažič, "Towards a standard approach for quantifying an ICT security investment", Computer Standards & Interfaces, Vol. 30, No. 4, 2008, pp. 216-222.

[7] ISO/IEC 27002:2005: Information technology — Security techniques — Code of practice for information security management.

[8] ISO/IEC 27005:2011: Information technology — Security techniques — Information security risk management (Second edition).

[9] NIST Special Publication 800-30: Guide for Conducting Risk Assessments, Rev. 1, September 2012.

[10] NIST Special Publication 800-39: Managing Information Security Risk, Organization, Mission, and Information System View.

[11] Siemens Enterprise, "The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures", 11 October 2005.

[12] NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1.0.

[13] N. Humaidi, V. Balakrishnan, "The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information", Proceedings of the 2nd International Conference on Management and Artificial Intelligence, Bangkok, Thailand, 7-8 April 2012, pp. 1-6.

[14] T. Takemura, M. Osajima, M. Kawano, "Economic Analysis on Information Security Incidents and the Countermeasures: The Case of Japanese Internet Service Providers", Advanced Technologies, pp. 73-89, InTech, 2009.

[15] H. Očevčić, K. Nenadić, K. Šolić, "Decision Support Based on the Risk Assessment of Information Systems and Bayesian Learning", Technical Gazette, Vol. 21, No. 3, 2014, pp. 539-544.

[16] T. Velki, K. Šolić, H. Očevčić, "Development of User's Information Security Awareness Questionnaire (UISAQ) – Ongoing Work", Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 26-30 May 2014, pp. 1564-1568.

[17] K. Šolić, T. Velki, T. Galba, "Empirical Study on ICT System's User's Risky Behavior and Security Awareness", Proceedings of the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 25-29 May 2015, pp. 1623-1626.