Towards a Hybrid Model for the Evaluation of Critical IT Systems

Davor Maček, Ivan Magdalenić, Nina Begičević Ređep
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
{davor.macek, ivan.magdalenic, nina.begicevic}@foi.unizg.hr

Abstract. *Given that today's very complex and interconnected business processes meaningly rely on Internet communication with other business entities, organizations are increasingly exposed to numerous security threats and imminent risks. Due to the lack of all relevant information and the time and resource constraints, it is not possible to collect and process all necessary information about an information system so that it can be adequately evaluated within an acceptable timeframe, which puts the organization into a state of increased security risk. By studying the relevant literature and existing models and techniques used in practice, it was determined that there is no solution to the stated problem of multicriteria decision-making in conditions of uncertainty in the domain of information security. Thus, the proposal is to design a model for more efficient (in terms of costs and time) decision-making on the security state of a critical information system by selecting the appropriate IT solution. In this paper we will present the iterative steps of DSRM (Design Science Research Methodology) for development of a new hybrid multicriteria model for the purpose of evaluation, ranking and selection of critical IT systems.*

Keywords. Information security, risk assessment, multicriteria decision-making, hybrid model

1 Introduction

Unavailability of the information system or any part of it may be caused by equipment failure, improper configuration or inadequate management. Also, there are notable external factors like emerging cyber attacks on organizations, particularly financial institutions and their clients (Biancotti, 2017; Bouveret, 2018; Raghavan and Parthiban, 2014), where particularly dangerous WannaCry and Petya attacks should be highlighted (Hsiao and Kao, 2018; Aidan et al., 2017). There has been a significant increase of security threats and cyber attacks on financial institutions, so according to Verizone Institute (Data Breach Investigations Report, 2020), as many as 86% of successful cyber attacks (i.e. breaches) were financially motivated, and according to the International Monetary Fund (Lagarde, 2018), the risk of cyber attacks is recognized as the most significant one in the financial sector.

Today's business of financial institutions relies heavily on communication over the Internet with their clients and other business entities, so banks are in fact increasingly exposed to numerous security threats and unavoidable risks. Assessment and management of IT security risks is a critical process. It's a set of related activities to control and manage risks of the information system. The main goal of this process is to reduce risks to an acceptable level (NIST SP 800-30; NIST SP 800-37), depending on the level of risk appetite which the organization's management is willing to accept (Mbowe et al., 2014). It is precisely the task of security professionals to enable the organization to operate in such conditions of uncertainty, i.e. risk.

Due to the rapidly growing trend of increasing security threats and newly discovered vulnerabilities and very often insufficient amount of time and other resources in organizations to effectively respond to risks, addressing the most critical ones and consequently assessing security countermeasures, controls and critical IT systems becomes an essential problem. Thus, the following research questions arise:

- Q1: How to enable more efficient decision-making on the security posture and the selection of appropriate critical information systems in a financial institution?
- Q2: Which elements of security risk analysis and assessment are appropriate and relevant for the development of a hybrid multicriteria model for the assessment and selection of critical information systems in order to more effectively make informed decision about the observed critical IT system in a financial institution?

- Q3: For which critical information systems is the proposed hybrid multicriteria model applicable and valid?

Therefore, the planned research deals with the issue of information security risk management in the field of critical information systems in a financial institution in the context of selecting an appropriate IT solution, all using multicriteria decision-making (MCDM) methods, in order to reduce risk to an acceptable level.

2 Related Work

The research initiative stems from the experience where the author identified a problem in the absence of an effective (in terms of costs and time) method or model for the assessment of critical information systems in a financial institution in order to better address security risks and make an appropriate decision on the security posture of the observed system, and then finally help in choosing an adequate IT solution. In order to provide answers to the research questions, it is necessary to make an analysis of the literature and existing models and methods in the areas of multi-criteria decision-making and risk management, which are used for the evaluation of IT systems.

By searching scientific citation databases, the following relevant papers were found on the topic of risk management and application of methods for multi-criteria decision-making for the purpose of evaluation and ranking of information systems:

In their paper (Fenz et al., 2014), the authors reviewed and compared current approaches to risk management, noting that they do not provide explicit mechanisms to support decision makers in developing risk management strategies in relation to cost trade-offs. So, as a result of the comparison, an abstract methodology was created in order for the problem to get aligned with the identified solution according to its generic phases.

According to (Barker, 2014), the gap between perceived and actual risk is extremely large. Although the vast majority of senior management claims that their cyber programs are effective, the number of significant security incidents and breaches of the information system with serious consequences for the company's operations is growing, with the financial damage also increasing.

According to (Wangen et al., 2018), a framework for evaluating the integrity of information security risk assessment methods is proposed, where a comprehensive comparison of ISRA (Information Security Risk Assessment) methods was conducted, representing a new framework developed using the DSR (Design Science Research) methodology. Taking into account only three aspects of observation, namely risk identification, estimation and evaluation, it was concluded that ISO / IEC 27005 is actually the most complete method.

In research (Maček et al., 2011), two methods for risk analysis and assessment are combined together, where the VECTOR method initially served to prioritize critical assets while later on OCTAVE-Allegro method is used for more detailed analysis, assessment and proposals for dealing with critical risks. Research has shown that the proposed ISRA methods are complementary and can be used sequentially, but there is still a problem of risk quantification.

In his work (Smojver, 2011), the author systematized and ranked international standards and methods for risk analysis and management, where the ENISA ranking list of ISRA methods was used as an input parameter. But the ENISA list is actually not complete and can be considered obsolete because some recently developed methods are not included.

In their research studies (Anikin, 2015; Hongsheng, 2015; He and Xin, 2016; Huang and Sun, 2018), the authors finally proposed the use of multicriteria decision-making methods (dominantly AHP) for the purpose of information security risk assessment, which can serve as certain guidelines and basis for developing a future hybrid multicriteria model for evaluating of critical IT systems.

ISRA is recognized as a vital method for identifying and prioritizing information assets, but in these papers or industry standards related to information security risk analysis and management, no frameworks or methods are found to effectively assess the security posture of an IT system using multicriteria decision-making in a way to select an appropriate solution in order to reduce risk to the organization.

Although there is a relatively significant number of publications on threats, vulnerabilities and associated risks and also relevant scientific papers in the field of multicriteria decision-making, a systematic review of index citation databases (Maček et al., 2020) shows that there is still no method or model based on solid mathematical foundations for assessment, ranking and selection of critical information systems combining methods for multicriteria decision-making with methods (or elements) for information security risk analysis and assessment. Thus, the observed problem is also interesting from the perspective of scientific research.

3 Proposal for a Hybrid Model

Given that there are many elements influencing the decision on an IT solution where time and other resource constraints become key challenges, a complex problem of multicriteria decision-making in conditions of uncertainty, i.e. risk in the field of information security, has been identified.

There are two general goals to be satisfied with the further research:

(1) Development of a new hybrid multicriteria model for more efficient decision-making on

the security posture and selection of an appropriate critical information system in a financial institution.

(2) Increasing the productivity and quality of the assessment process of critical IT systems.

By creating a new hybrid multicriteria model with elements for risk analysis and risk assessment and thus satisfying the first general objective, consequently the answers to research questions Q1 and Q2 are also given. The second general objective is satisfied when applicability, validity and efficiency of the new model is proven with relevant case studies, and thus also giving the answer to research question Q3.

After defining the research questions and the goals, it's also necessary to present the generalization of a possible solution to the observed problem, which is actually stated as a recommendation in the first phase of DSRM methodology. The generalization of the model itself is necessary in order to get a better overview of what is actually to be done and with which elements of the model.

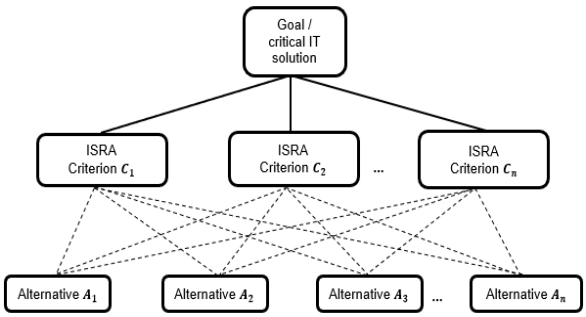

Figure 1. Generic conceptual model

In Fig.1, a generic conceptual model is presented where the goal is to assess, rank and choose the appropriate critical IT solution among the given alternatives which best fits security needs, and where information security risk assessment elements are used as evaluation criteria. On this occasion, the generic conceptual model is presented in the form of a hierarchy for simplification and easier understanding of the issue, while the final model will also include a network structure due to interdependencies and influences between elements for information security risk analysis and assessment.

The motivation for the planned research is to further deepen the knowledge on the application of ISRA and MCDM areas, and to discover the opportunities for more efficient decision-making on critical information systems with the necessary reduction of risks to the organization. The analysis of specific problems related to the selection of a particular security IT solution or a critical element of the information system in conditions of uncertainty (risk) leads to the problem of generalization.

The intention of the research is to collect empirical data, the analysis of which should improve the knowledge about the selection of critical IT systems in conditions of risk. Based on this knowledge, it is planned to develop a new model for more efficient decision-making on the security posture and the selection of a critical IT solution in the organization, which is actually the main goal of the research.

The model should enable the assessment of critical information systems using multicriteria decision-making methods, where attributes from the relevant methods for risk analysis and assessment will be used as evaluation criteria. Since the hybrid model will use generic criteria for IT risk assessment with the purpose of systems' evaluation, that actually presents a novelty given that the criteria inherent in the subject of evaluation are traditionally used. The new hybrid multicriteria model should be more efficient in terms of costs and time.

The target group of solutions for the application of a new hybrid multicriteria model are critical information and security systems in a financial institution, e.g. network security systems, cryptographic systems, online transaction systems, identity and access management systems, cloud services, etc.

4 Research Methodology

The research paradigm that will be followed in this research is called Design Science Research Methodology (DSRM) (Peffers et al., 2007), which is used for research purposes primarily in engineering and information systems. Research using this paradigm involves creating new knowledge by designing new or innovative artifacts. Artifacts can include algorithms, computer interfaces, system design methodologies or languages, and models. Researchers in design science can be found in many disciplines and fields, especially in engineering and computer science, using a variety of approaches, methods, and techniques (Peffers et al., 2007). In this particular case, the artifact that aims to solve the identified problem is a new hybrid model for evaluating, ranking and selecting IT solutions or critical security elements of an information system in a financial institution using multicriteria decision-making with elements for analysis and assessment of information security risks. According to the guidelines for the implementation of design based research (Hevner, 2007), it is planned to conduct an additional activity in the research methodology. It' about creating a knowledge base where the goal is to conduct a detailed review of research areas and show that there is currently no solution to the research problem.

After explaining the observed problem and defining the goals and research questions, the research continues by applying the method of systematic literature review, SLR (Kitchenham, 2007). SLR is a formalized and repeatable process to document relevant knowledge in a particular subject area. This method is currently considered the best for domain review and a prerequisite for objective method

selection. In the planned research it will be used as a means of evaluating and interpreting available studies from defined domains (ISRA and MCDM) in order to create a knowledge base that will serve as a reference point for the new model.

This research phase has been already conducted and the relevant results are presented (Maček et al., 2020). Due to the complexity of the research topic which includes two interdisciplinary domains, namely risk management and multicriteria decision-making, the literature search was done on the most important scientific citation databases that were available to the authors during the research period. A systematic literature review has determined which methods for multicriteria decision-making would be suitable for the development of a new hybrid model and its validation in case studies in the field of critical IT systems.

A review of the literature showed that in many analysed studies some kind of quantification was searched for the assessment and ranking of IT security risks, risk factors or software solutions, and thus the use of some of the quantitative MCDM methods was required. The survey showed that the international industry standard ISO/IEC 27005 (with different release years) was dominantly analysed and used for the purposes of information security risk analysis, assessment, treatment and management. Other widely accepted ISRA standards and methods are OCTAVE, NIST SP 800-30, CORAS, CRAMM and ISO/IEC 31010:2009. Also, the survey discovered the frequency of application of MCDM methods and techniques in ISRA domain, where the predominantly used MCDM method for the purposes of IT security risk analysis and assessment is the AHP. This could be attributable to the relative ease of application of the AHP itself and its great popularity among researchers. Other frequently used MCDM methods in the ISRA domain are the ANP, DEMATEL and TOPSIS. The DEMATEL technique is used to calculate the influence weights, while the ANP is used to calculate interdependencies of the elements. This is very important roadmap and has a strong impact for the further research to extend the core ISRA elements, define their mutual influences and interdependencies, and integrate those elements within one (or even more) of the MCDM methods in order to make an evaluation of the critical IT systems in a more efficient way. Additionally, the SLR has revealed a trend in development of hybrid models for risk analysis, for determining on the security posture or selecting an appropriate IT system by using multicriteria decision-making.

The next qualitative research step is to conduct a survey among IT security professionals regarding the domain of information security risk assessment. Previous research has shown that currently none of the most significant ISRA methods fully meets the requirements of comprehensiveness and complementarity of its attributes for risk analysis and assessment with any of the MCDM methods. The earlier solution proposal was found in the form of the simple VECTOR method for risk ranking and prioritization obtained by the author's preliminary research (Maček et al., 2012; Maček et al., 2017). But, the VECTOR method itself is very rarely used and is not proven with the relevant number of studies. Thus, it becomes necessary to conduct a research where from the most common ISRA methods the most relevant attributes used in the process of risk analysis and assessment will be extracted. It's planned to examine experienced IT security experts from various countries and different financial institutions holding relevant industry certifications (e.g., CISSP, CISM, CEH, etc.). The results obtained in this phase of the research will be used for input and development of the knowledge base and later on as input parameters (i.e. generic elements) of the new hybrid multicriteria model. The Delphi technique is intended to be applied in this research phase, and the survey form will be distributed to the research participants via e-mail.

Based on previous phase and defining the necessary knowledge base, the next step is to move to the design and development phase of the model for more efficient decision-making on the evaluation, ranking and selection of a critical IT solution in a financial institution in conditions of uncertainty (risk). In order for the new model to be developed and tested, it is necessary to provide certain prerequisites and point out the assumed limitations of the model itself:

- Development of a conceptual model: Before creating a final model based on research of ISRA and MCDM methods, it is necessary to set a specific conceptual model, i.e. try to make a generalization.
- Complementarity: Selection of appropriate, i.e. complementary methods and elements for risk assessment and multicriteria decision-making. Given the number of existing methods, techniques and tools in both observed research domains, namely risk management and multicriteria decision-making, the challenge is certainly to find exactly those complementary (i.e. their elements) that solve the observed complex problem in the most efficient way, and with the purpose of which the creation of the knowledge base was conceived.
- Generic attributes: In order to obtain a standard model that enables more efficient solution of the identified complex problem, generic risk criteria for the evaluation of critical IT systems are a kind of limitation in terms of flexibility of the model and its application to only certain segments in the field of IT security in the financial sector.

The design and development phase is followed by a case study to demonstrate and evaluate the designed model in order to verify the applicability and usefulness of the model itself on critical IT systems in a financial institution. The evaluation of the model will be done in collaboration with information security experts, as well as in the previous DSRM phase. The

case study will include 2 process steps of the DSRM methodology: demonstration of a new hybrid model and evaluation of the same. The aim of the first phase of the case study is to demonstrate the applicability of the new model on critical IT systems, while the aim of the second phase is to validate the model in order to see its usefulness. Validation of the model would be done by comparing the results obtained by applying a new hybrid multicriteria model using the inherent (common) attributes of a critical IT solution with the results of the target model using generic risk criteria.

Since the DSRM is a repetitive process, a calibration of the model is also foreseen in case of need in order to achieve additional efficiency. At the end of the validation process, data analysis will be done in the final research step which is conclusion and communication, with the following aims:

- Making a decision on achieving the main research goals
- Presentation of answers to research questions
- Proving or disproving hypotheses.

Table 1. DSRM phases and methods for development of a hybrid multicriteria model

DSRM phases	Methods used
Problem identification and motivation	Systematic observation of ISRA domain
Defining the objectives of a solution	Proposal of tentative design by generalization
Creating a knowledge base	• Systematic literature review (SLR) – analysis • Delphi survey for a panel of IT security experts regarding ISRA elements
Design and development	Synthesis of elements and modeling a new artifact, i.e. hybrid multicriteria model
Demonstration	Demonstration of the new model that is developed according to the inputs from the previous DSRM phases
Evaluation	• Case studies, comparisons and measurement in order to check applicability, validity and efficiency of the new model • Model calibration – iterate back to design and development phase
Conclusion and communication	Presentation of the solution, i.e. publication in the form of a scientific paper in a journal and doctoral dissertation communication

Table 1 represents a summary of DSRM phases and methods for development of a new hybrid model planned for use in the research. This also gives an additional scientific contribution in the context of the methodology along with the methods used for development of a new multicriteria model for evaluation of critical IT systems.

5 Conclusion

The following scientific contribution is expected from the proposed research, which arises from the defined research goals and used scientific methods:

- Developed new hybrid model with generic elements for risk analysis and assessment using multicriteria decision-making enables more efficient decision-making on the security posture of a critical IT system, and thus consequently enables a financial institution to better respond to security threats and risks by choosing an adequate IT solution.
- Systematization of knowledge and concepts on multicriteria decision-making methods that are suitable for application in the field of information security together with methods for risk analysis and assessment.

In addition to the expected scientific contribution, the proposed hybrid multicriteria model should be also practically applied in the financial industry for security professionals and especially for decision makers, which actually presents a broader social-economic contribution.

Acknowledgments

This work has been fully supported by the Croatian Science Foundation under the project IP-2019-04-4864.

References

Aidan, J.S., Verma, H.K., & Awasthi, L.K. (2017). Comprehensive Survey on Petya Ransomware Attack. *Proceedings of the International Conference on Next Generation Computing and Information Sciences* (*ICNGCIS*) (pp. 122-125). Model Institute of Engineering and Technology, Jammu, India. doi:10.1109/ICNGCIS.2017.30

Anikin, I. (2015). Information Security Risk Assessment and Management Method in Computer Networks. *International Siberian Conference on Control and Communications* (*SIBCON*). doi:10.1109/SIBCON.2015.7146975

Barker, K. (2014). The gap between real and perceived security risks. *Computer Fraud & Security*, 4, 5-8. https://doi.org/10.1016/S1361-3723(14)70478-6

Biancotti, C. (2017). Cyber Attacks: Preliminary Evidence from the Bank of Italy's Business Surveys. *Bank of Italy Occasional Paper*, 373. Retrieved from https://www.bancaditalia.it/pubblicazioni/qef/2017-0373/

Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *IMF Working Paper, International Monetary Fund*, 18(143). Retrieved from https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

Fenz, S., et al. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), 410-430. https://doi.org/10.1108/IMCS-07-2013-0053

He, M. & Xin, A. (2016). Information Security Risk Assessment Based on Analytic Hierarchy Process. *Indonesian Journal of Electrical Engineering and Computer Science*, 1(3), 656-664. Retrieved from http://ijeecs.iaescore.com/index.php/IJEECS/article/view/314

Hevner, A.R. (2007). A Three Cycle View of Design Science Research. Scandinavian Journal of Information Systems, 19(2), 87–92. Retrieved from https://aisel.aisnet.org/sjis/vol19/iss2/4

Hongsheng, L., et al. (2015). Information Security Risk Assessment Based on Two Stages Decision Model with Grey Synthetic Measure. *Proceedings of the 6th IEEE International Conference on Software Engineering and Service Science* (*ICSESS*). doi:10.1109/ICSESS.2015.7339176

Hsiao, S-C. & Kao, D-Y. (2018). The Static Analysis of WannaCry Ransomware. *Proceedings of the 20th International Conference on Advanced Communication Technology* (*ICACT*) (pp. 153-158). doi:10.23919/ICACT.2018.8323679

Huang, Y-L., & Sun, W-L. (2018). An AHP-based Risk Assessment for an Industrial IoT Cloud. *IEEE International Conference On Software Quality, Reliability And Security Companion* (*QRS-C*) (pp. 637-638). doi:10.1109/QRS-C.2018.00112

Kitchenham, B. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. *EBSE Technical Report*. Software Engineering Group, School of Computer Science and Mathematics, Keele University, UK, and Department of Computer Science, University of Durham, UK. Retrieved from https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.471

Lagarde, C. (2018). Estimating Cyber Risk for the Financial Sector. *IMFBlog, Insights & Analysis on Economics & Finance*. Retrieved from https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/

Maček, D., Magdalenić, I., & Ivković, N. (2011). Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods. *Proceedings of the 22nd Central European Conference on Information and Intelligent Systems* (*CECIIS 2011*), Information Systems Security, pp. 133-139. University of Zagreb, Faculty of Organization and Informatics Varaždin.

Maček, D., Magdalenić, I., & Ivković, N. (2012). Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard. *Proceedings of the 23rd Central European Conference on Information and Intelligent Systems* (*CECIIS 2012*), Information Systems Security, pp. 305-311. University of Zagreb, Faculty of Organization and Informatics Varaždin.

Maček, D. & Alagić, D. (2017). Comparisons of Bitcoin Cryptosystem with Other Common Internet Transaction Systems by AHP Technique. *Journal of Information and Organizational Sciences*,41(1),69-87. https://doi.org/10.31341/jios.41.1.5

Maček, D., Magdalenić, I., & Begičević Ređep, N. (2020). A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment. *International Journal of Safety and Security Engineering*, 10(2), 161-174. https://doi.org/10.18280/ijsse.100202

Mbowe, J.E., et al. (2014). A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy. *Journal of Information Security*, 5(4), 166-177. doi:10.4236/jis.2014.54016

NIST SP 800-30: Guide for Conducting Risk Assessments, Joint Task Force Transformation Initiative, Rev. 1. (2012). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST SP 800-37: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Joint Task Force, Rev. 2. (2018). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Peffers, K., Tuunanen, T., Rothenberger, M.A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45–78. https://doi.org/10.2753/MIS0742-1222240302

Raghavan, A.R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research and Academic Review*, 2(2), 173-178. Retrieved from http://www.ijcrar.com/archive-6.php

Smojver, S. (2011). Selection of information security risk management method using analytic hierarchy process (AHP). *Proceedings of the 22nd Central European Conference on Information and Intelligent Systems* (*CECIIS 2011*). University of Zagreb, Faculty of Organization and Informatics Varaždin.

Verizon Enterprise (2020). Data Breach Investigations Report, Public Sector Excerpt. Retrieved from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17, 681-699. https://doi.org/10.1007/s10207-017-0382-0