Decision support systems for cyber risk management

Aurelian Buzdugan[1], Gheorghe Capatana[2]

Abstract

In this paper we will outline the results of the literature review on use of decision support systems for cyber risk management in critical infrastructures. We will briefly present the identified research goals as well as the opportunity of using the support systems by decision makers and operators. Based on the elements that we have identified so far, as well as the analysis of previous research, we will draft a conceptual design on the use of decision support systems for managing cyber risks. We will outline the previous results on this topic and propose future steps on developing a proof of concept.

Keywords: decision support systems, cyber security, risk management, critical infrastructures.

1. Introduction

Decision making process has become more complex with the growing amount and complexity of data, as well as short time required in making a decision. This is also applicable in the activities of managing cyber risks in critical infrastructures, where data sets consisting of risks, implications and mitigations have to be assessed in order to aid the decision makers and operators. Existing approaches in risk management are general and cover different types of risks, however are not fully focused on the cyber security risks. The emergence of IT components in almost all sectors of the industry, creates new types of risks that require specialized knowledge and understanding of the systems in order to assess, evaluate and apply adequate mitigating controls.

The developments in the past decade have led to a new state of the context driving IT systems, where the number of decision-making

© 2020 by Aurelian Buzdugan, Gheorghe Capatana

activities has increased, the problems became more complex as well as the need for computer aided tools has become a necessity [3].

This sets the premises upon which we ascertain that decision support systems (DSS) are adequate solutions for managing cyber risks in critical infrastructures.

2. Current status of DSS use in cyber risk management

In previous papers we have reviewed existing scientific literature on the use of DSS in cyber risk management [1]. The main results show that this type of systems has not been fully explored in cyber risk management and we proposed future research goals in this direction. Among the highlights, we noticed a focus on elements such as resilience and contextual awareness, denoting the importance of these factors in the critical infrastructure domain.

This contributes to the idea that a holistic approach is required in order to identify and propose a concept of using DSS for our scope, where domain specific elements need to be taken into consideration. We have also observed that:

- All papers focus on a concept of DSS, however none was yet proven in practice.
- Various concepts and algorithms were embedded in the DSS, such as Bayesian networks or ontology description of actions.
- Actions such as modelling, categorization and correlation were common in the system descriptions.
- No DSS focused on cyber risks has been identified yet.

The critical infrastructure domain is one that does not have extensive coverage in the use of DSS. We believe that dedicated DSS for cyber risk management would be a novelty, as well as a modern solution for the emerging risks.

There are specific requirements that have to be taken into account when developing a concept, and mainly in terms of target users. In critical infrastructures we foresee both operators as well as decision makers making use of the risk mitigations and recommendations created by the DSS. Therefore, the data analyzed could considerably grow, as it needs to include both strategic as well as technical details. Respectively, the output data will be adjusted and formatted based on the target users.

We believe that a concept of DSS for managing cyber risks would support the existing research in this type of systems, and also integrate other emerging disciplines such as machine learning, artificial intelligence and data mining.

Incidents or events related to the physical aspects of a critical infrastructure, such as theft, intentional damages or natural hazards were the focus for years in the risk management process. Certain frameworks and systems for supporting risk management in the identification, assessment and evaluation of risks have been developed, however these in our opinion do not cover exhaustively the emerging risks such as cyber security risks. Our goal is to explore how DSS explicitly focused on cyber risks could be developed in this context. Taking into account that generic risk management frameworks exist, having DSS as interoperable modules would make this concept likely to be adopted and implemented. This is also supported by the fact that developing DSS for all types of risks could be time and resource consuming.

We believe that the conceptual DSS can be also assumed to be a type of version 8.0 [2], which will be built using computer cognitive systems, and making use of cloud and mobile computing [3]. We would like to add the potential of using artificial intelligence in certain processes, such as searching the best solution, or identifying interdependencies and modelling of the system state after a proposed action would be taken.

The response time, taking into account the peculiarity of risk management and then the response, should be as swift as possible. The design should accommodate multi-participant use, as risk management is an organizational issue. The same applies to cyber risks, where at least decision makers and operators are involved, and potentially third parties as well [4]. The multi-participant model, as per Nunamaker, ensures that requirements such as parallelism and anonymity would also be part of the design. These can be applied to multiple use cases, such as cooperating on the risk mitigation, either gathering input on potential mitigation measures from both internal, as well as external sources.

3. Conclusion

We believe DSS possess adequate abilities to help tackle emerging cyber risks in the critical infrastructure domain. The features, concepts and

technologies used by a modern DSS are an opportunity in support decision makers by analyzing large and complex sets of data and extracting relevant data.

The future goals are to develop the architecture of the proposed type of DSS for managing cyber risks in critical infrastructures. This would improve the overall process of managing cyber risks in this domain.

This concept highlights a potential application of DSS for cyber risk management in critical infrastructures. The previous results, combined with the conceptual features of the DSS, constitute a baseline for a future DSS for our scope. The insights gained serve as input for the future research agenda and will be integrated in the architecture of a decision support system.

References

[1] A. Buzdugan. *Review on use of decision support systems in cyber risk management for critical infrastructures*, Journal of Engineering Science, vol. XXVII, no. 3, 2020, pp. 134 - 145, DOI: 10.5281/zenodo.3949684.

[2] D.J. Power and G. Phillips-Wren. *Impact of social media and Web 2.0 on decision-making*. J Decis Syst, 20(3), 2011, pp. 249–261.

[3] F.G. Filip. *DSS—A Class of Evolving Information Systems*. In: Dzemyda G., Bernatavičienė J., Kacprzyk J. (eds) Data Science: New Issues, Challenges and Applications. Studies in Computational Intelligence, vol 869. Springer, Cham. 2020, https://doi.org/10.1007/978-3-030-39250-5_14.

[4] G.L. Kolfschoten and J.F. Jr. Nunamaker. *Organizing the theoretical foundation of collaboration engineering.* In: Collaboration systems: concept, value, and use. Routledge, Taylor and Francis Group, London, 2015, pp 27–41.

Aurelian Buzdugan[1], Gheorghe Capatana[2]

[1]Moldova State University
E-mail: aurelian.buzdugan@yahoo.com

[2]Moldova State University
E-mail: gh_capatana@yahoo.com