A cybersecurity risk assessment

Valentina Petrova
Nikola Vaptsarov Naval Academy, Varna, Bulgaria
vmb75bg@gmail.com

Abstract: *The main purpose of this paper is to offer a data-driven approach to assess cyber risk and to ensure appropriate confidentiality, integrity, and availability. A study presents the decision hierarchical model of cyber security risk assessment based on AHP methodology and describes a quantitative measure for evaluating and ranking security incidents. It can be used to conduct cost-benefit analysis, design and optimize cybersecurity in the systems.*

KEYWORDS: CYBERSECURITY, AHP

1. Introduction

Cyber risk assessment requires defined and objective methodologies; otherwise, its results cannot be considered reliable. Too much subjectivity in the risk assessment process can weaken the credibility of the assessment results and compromise risk management programs [7, 13].

Defining reliable models for the cyber risk exposure is still an open problem. Existing models [1, 12] suffer from some important concerns that, for example, prevent the insurability market development [1].

This study presents a cybersecurity model to conduct a cybersecurity risk assessment. It demonstrates how to use AHP to perform risks assessment to prioritise risks in the systems. AHP risk assessment methodology is discussed extensively including how to structure risks in a hierarchy, make pair wise comparison to assess which cybersecurity risk is more important and calculate priority weight of the risks to organize risk ranking.

AHP methodology produces quantitative cybersecurity risk ranking which helps to prioritise the components of a system in terms of their level of vulnerability to an attack, and threats in terms of the danger they pose. Risk assessment assists the engineers with the development of security policies, with the design of secure system and with the rational allocation of scarce resources. It facilitates the communication between security, business and experts.

2. A multi-criteria decision-making approach

Cyber risk evaluation and the study of its related impact are performed mostly in qualitative ways, which are usually affected by errors and misrepresentations of the risk. They also exhibit several disadvantages, such as the approximate nature of the achieved results and the difficulty of performing a cost-benefits analysis [7]. The lack of quantitative data can be dangerous: if the assessment is entirely qualitative, subjectivity will loom large in the process [13].

This has created a multi-criteria problem, which can be solved using a multi-criteria decision making approach (MCDM) [4].

Table 1 Summary of applications of the DM techniques [3]

Method	Application	Percentage
AHP	128	32,57%
ELECTRE	34	8,65%
DEMATEL	7	1,78%
PROMETHEE	26	6,62%
TOPSIS	45	11,40%
ANP	29	7,38%
Aggregation DM methods	46	11,70%
Hybrid MCDM	64	16,28%
VIKOR	14	3,56%

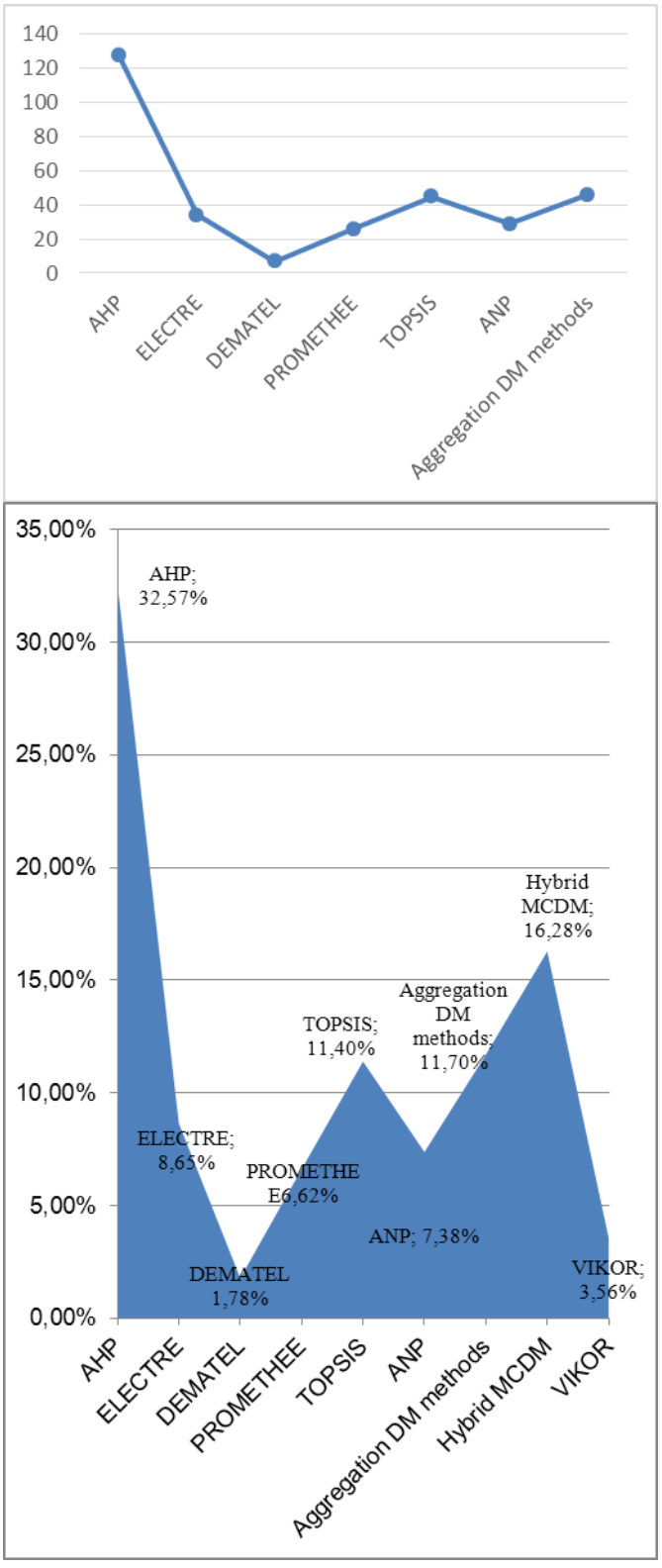

Fig. 1 Frequency of MCDM techniques and approaches

The selection process is based on a literature review and classification of international journal articles [3]. MCDM provides strong decision making (DM) in domains where selection of the best alternative is highly complex. MCDM method has been applied to many domains to choose the best alternatives. Where many criteria have come into existence, the best one can be obtained by analysing different scopes of the criteria, weights of the criteria, and the selection of the optimum ones using any MCDM techniques. Table 1 shows frequency of MCDM techniques and approaches. Based on the results presented in this table, a total of 393 studies have employed DM techniques and approaches. Table 1 and fig. 1 shows that AHP method (32.57%), and its applications have been used more than other tools and approaches.

AHP uses objective mathematics to process subjective preferences of a risk manager or a risk management group in determining the relative importance of risks [11].

3. An Analytical Hierarchy Process for cyber security risk assessment.

The process of risk assessment and treatment is fundamental to the implementation of an effective cyber security program and plays a crucial role for the national and international regulations in the field of data protection [7, 13].

The confidentiality, integrity and availability are considered the core underpinning of cyber security and the steps for achieving them are: determination of the affecting criteria, questionnaire collection and statistical analysis, weighting these criteria, evaluation of the entire performance according to these weighted criteria. The evaluation criteria used in this study are: attacks, vulnerabilities, penetration testing, threats, assets, security measures, unauthorized access, and security alerts. According to giving priority to criteria weight, the application allow to find best choice (Availability) and worst choice (Integrity) from all results shown in fig. 2.

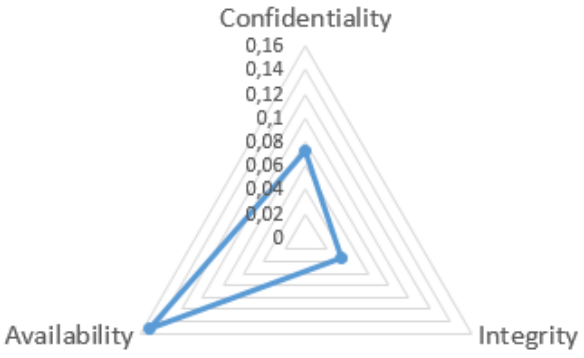

Fig. 2 Comparison of the alternatives

If the stakeholders' answers are evaluated with a more objective process, this will result in a more objective profiling of the company [7, 13]. This is the aim, which the author pursue by introducing the use of some data-driven key risk indicators.

Data-driven key risk indicators suppose that the author disposes a tool that monitors the company and returns a sufficient amount of quantitative evidences such as malicious code / software activity (i.e., malware, ransomware, botnet evidences); insecure / unencrypted / vulnerable protocols usage (i.e., P2P, vulnerable SSL, etc.); deep web exposure (company targeted by criminals); data breaches due to human errors, third parties, or hacking activity; software / infrastructure vulnerabilities [7, 13].

Quantitative risk assessments based on subjective criteria are effective when experts use:

- indicators and incidents to feed data into models;
- a vulnerability scale assesses and indicates how well prepared we are for a cyber risk event;
- measures for following factors: availability, frequency, confidentiality, integrity, and probability of a cyber risk occurring.

Cyber risks will be quickly rated on their potential impact.

An Analytical Hierarchy Process (AHP) represents the field of science called MCDA (Multi Criteria Decision Analysis), which is intended to assist the users in making decisions, defined as a subjective measurement of various preferences [9]. The main goal of the AHP method is dealing with complex decisions by giving them a rational structure, calculating the weight of the criteria and alternatives.

The AHP method is composed by the following stages:

Stage 1: The AHP was used to determine critical and vulnerable cyber security risks within systems based on a decision goal, criteria list and alternatives. The situation is to assess all cyber security risks and to prioritise inherent risks.

Goal: Identifying critical substations and estimating cyber security risks.

Criteria: The author proposed eight criteria named attacks, vulnerabilities, penetration testing, threats, assets, security measures, unauthorized access, and security alerts.

Alternatives: The alternatives are Confidentiality, Integrity, and Availability.

The confidentiality, integrity and availability are considered the core underpinning of cyber security. Security control and vulnerability can be viewed in light of one or more of these key concepts.

Stage 2: The decision hierarchical model of cybersecurity risk assessment

The criteria and alternatives are organized in a hierarchy. The hierarchy has three levels. The first level is the decision goal, the second level is the risks and the third level is the alternatives.

The hierarchical structure is defined and described to support cyber security. The complete hierarchical structure is illustrated in Figure 3:

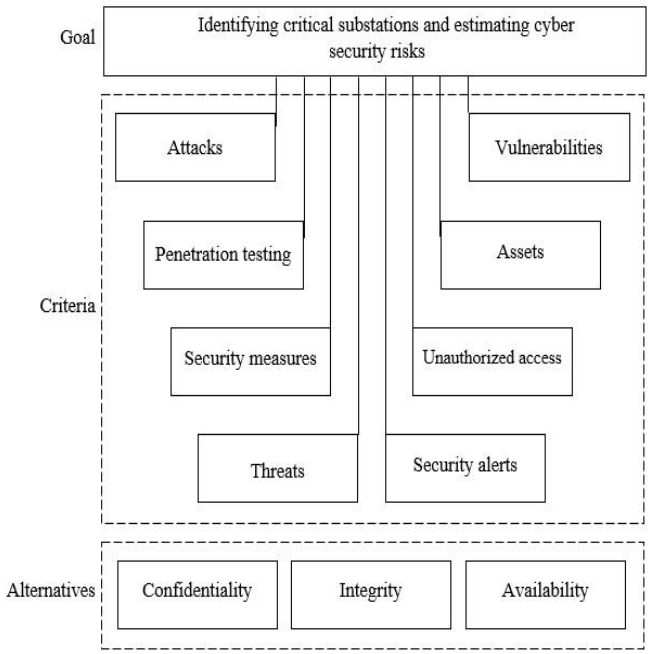

Fig. 3 The decision hierarchical model of cybersecurity risk assessment

The author presents the decision hierarchical model of cyber security risk assessment to evaluate and rank security incidents using the AHP whereby the eight decision criteria were the likelihood of an event and its consequences. The model reduces the

number of risks and allows security analysts to focus on a critical incidents, which reduces the time and resources.

Stage 3: Mathematical implementation of the method Analytical Hierarchy Process.

Analytic hierarchy process (AHP) is a method of decision making using objective calculations based on evaluation of several criteria [10]. The AHP defines some stages of analysis [2, 6]: the hierarchical structures formulation, prioritization, priority weight calculation of each criteria or alternative, and consistency checking. The hierarchical structure is defined by considering the scope, objectives, criteria, relevant actors, and alternatives [10]. Priority is a value that determines the level of importance of an alternative or criteria [2]. AHP uses pair wise comparisons to assess the cybersecurity risks. The AHP defines pairwise comparison to determine priorities using a matrix to compare variable of the same level in pairs. Risk assessors decide which risk is more important and decide the strength of importance using a scale of 1 to 9. Comparisons were implemented using the Saaty preference scales [10]. Table 2 presents the comparison scale.

Table 2 Scale of the AHP Method [9]

Verbal Expression	Explanation	Scale	Reciprocal values
Equal importance	Two activities contribute equally to the objective.	1	1.000
Moderate importance	Experience and judgment slightly favour one activity over another.	3	1/3 (0.333)
Strong importance	Experience and judgment strongly favour one activity over another.	5	1/5 (0.200)
Very strong importance	An activity is favoured very strongly over another.	7	1/7 (0.143)
Extreme importance	The evidence favouring one activity over another is of the highest possible order of affirmation.	9	1/9 (0.111)
Intermediate values	The values are compromises between the previous definitions.	2 4 6 8	1/2(0.500) 1/ 4 (0.250) 1/6 (0.167) 1/8 (0.125)

Priority weighting of each criteria or alternative is calculated using the Eigen value principle [4]. This can be defined as a geometric mean method. The accuracy of the decisions is measured by computing consistency ratio (CR) and Consistency Index. Consistency checking is performed to determine the likelihood of conflicting inputs. The inconsistency value should not be more than 10% [10].

All proposed criteria were accepted as important, but four of them were ranked above the average mark. These criteria are: attacks, vulnerabilities, threats, and assets. The final ranking of alternatives are shown in structured evaluation of confidentiality, integrity, and availability relative to the importance of the criteria in Figure 4.

According to some criterion, confidentiality is more advantage than the other alternatives. The result demonstrates that confidentiality is the most appropriate that meets the criteria.

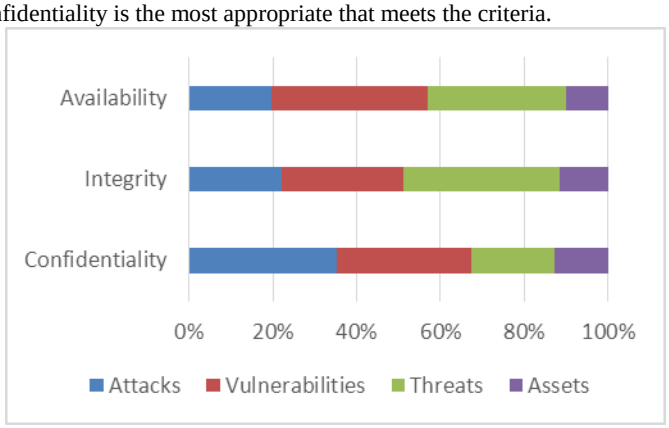

Fig. 4 Structured evaluation of confidentiality, integrity, and availability relative to the importance of the criteria

4. Conclusion

The author introduced the ASP methodology and described how it could be used to derive a quantitative measure for the cybersecurity risk assessment.

AHP methodology quantifies a cybersecurity risk assessment, helps to prioritise the components of a system in terms of their importance to the successful operation of the system, and improves subjective judgement by providing consistency in the cybersecurity risk assessment process.

A cyber security risk assessment methodology that may be exploited in the process of the design of instrumentation and control systems is suggested. The methodology outlines eight criteria that must be undertaken in order to conduct cyber security risk assessment during the system and component design, and equipment supply three stages. The paper describes the activities that must be undertaken during each stege.

This research recommends using more criteria in the future, and further integration of the method with other MCDM techniques and fuzzy methods to select and rank the best alternatives based on the identified criteria.

As subjects of future work are: vulnerabilities within the system will be identified and quantified using the Fuzzy Evaluation Method. An attack graph will be designed and used in order to find cyber scenarios, the probabilities of which will be also calculated.

5. References

1. Biener, C. ,M. Eling, and J. H. Wirfs, "Insurability of cyber risk: an empirical analysis," The Geneva Papers on Risk and Insurance—Issues and Practice, vol. 40, no. 1, pp. 131–158, 2015.

2. Ishizaka A., P. Nemery, Multi-criteria decision analysis methods and software, Chichester: John Wiley and Sons, (2013).

3. Mardani A., A. Jusoh, K. Nor, Z. Khalifah, N. Zakwan, A. Valipour, Multiple criteria decision-making techniques and their applications – a review of the literature from 2000 to 2014, Economic Research-Ekonomska Istraživanja, 2015.

4. Muhammad N., N. Cavus. Fuzzy DEMATEL method for identifying LMS evaluation criteria. 9th International Conference on Theory and application of Soft Computing, Computing with Words and Perception, 2017.

5. Naumov S. and I. Kabanov, "Dynamic framework for assessing cyber security risks in a changing environment," in Proceedings of the 2016 International Conference on Information Science and Communications Technologies (ICISCT), pp. 1–4, Tashkent, Uzbekistan, November 2016.

6. Petrova V., Using the Analytic Hierarchy Process for LMS selection, CompSysTech '19: 20th International Conference on

Computer Systems and Technologies, June 2019, Ruse, Bulgaria, Pages 332–336, ISBN: 978-1-4503-7149-0.

7. Rot, A., "IT risk assessment: quantitative and qualitative approach," in Proceedings of the World Congress on Engineering and Computer Science 2008 (WCECS 2008), San Francisco, CA, USA, October 2008.

8. Saaty, T.L., 1980. The Analytic Hierarchy Process. McGraw-Hill, New York.

9. Saaty T., Theory and Applications of the Analytic Network Process, RWS Publications, 2005.

10. Saaty T., L. Vargas, Models, methods, concepts, and application of the analytic hierarchy process, New York: Springer, 2012.

11. Sum, R., Risk Prioritisation Using The Analytic Hierarchy Process. Innovation and Analytics Conference and Exhibition (IACE 2015)AIP Conf. Proc. 1691, 030028-1–030028-8; doi: 10.1063/1.4937047

12. Ugur Aksu M., M. Hadi Dilek, E. Islam Tatli et al., "A quantitative CVSS-based cyber security risk assessment methodology for IT systems," in Proceedings of the 2017 International Carnahan Conference on Security Technology, pp. 1–8, ICCST, Madrid, Spain, October 2017.

13. https://doi.org/10.1155/2019/6716918