INFORMATION SYSTEM FOR CYBER SECURITY MATURITY ASSESSMENT

CZU: 004.056.53

Aurelian BUZDUGAN

Doctoral School of Physical, Mathematical, Information and Engineering Sciences, Moldova State University

Cyber risk management for critical infrastructure is a current research topic due to the actuality of cyber threats in this domain. The number of attributes and dimensions that have to be taken into account require computer assisted decision making, to improve the efficiency and resources spent for this process. We proposed a model to evaluate the cyber security maturity in critical infrastructures [1], which was built with the scope of estimating the efficiency of a decision support system to be used for this task [2]. In this paper we present an application proof of concept for operationalizing this model in large organizations. We implemented the basic functionality for assessing the cyber security maturity based on the existing knowledge from the proposed model. The application is expandable and can be integrated and adjusted to the need of any organizations.

Keywords*: cyber security maturity model, knowledge base, application, decision making.*

Cyber security maturity assessment is a complex topic due to the interdependence of attributes from various dimension. The connection between organization's management style, technical systems, education and training of users as well as human factor elements are directly related to the cyber security stance of an organizations. We developed and proposed a model for assessing the cyber security maturity based on 4 dimensions and 16 attributes [1, 2]. The results of this model show the estimated efficiency of an information security system used for cyber risk management. In addition, the model is multidimensional and can also be used to identify areas that require attention in order to improve the cyber security stance. In addition, a comparative analysis with ISO27001 has shown that the selected attributes can also be used in the support of ISO27001 Governance assessments, as these can characterize the overall management of cyber security in the organization. This increases the rate of efficiency and potential use cases where this model can be applied. In order to improve the usability and integration of the model in any type of organization, we have developed a proof of concept application that automates the assessment process and facilitates the review of final results.

In this paper we present the program used to implement the model to evaluate cyber security maturity in a critical infrastructure. The programming language selected is Python, due to the versatility as well as ready made packages. This improves the reading and adaption of the code, as well as it a commonly used language for this scope.

The program contains one class named *Model*, that covers the model implementation, and one class named *UserInterface*, responsible for the overall interface and end-user interaction such as menu creation, visualization and data input. In *Python*, classes provide an easy way of combining data, functionalities and methods, hence this solution can be easily understood and adapted as needed. After instantiation, classes can be used throughout the program. As we focused on modularity and interoperability, we decided this approach the best solution for this goal.

Level	Criteria	Element	Attribute
Very High	*pol_adm*	1	The requirements for cybersecurity and resilience are taken into account in the design and evaluation phase of the system and are recognized as the combination of technology and the human dimension.
Very High	*pol_adm*	2	In the decision-making process, cybersecurity and the resilience factor have a higher weight compared to costs.
Very High	*pol_adm*	3	Responsibilities for cyber security are clear and well defined according to the respective structure and functions. The information exchange process is well established vertically and horizontally, including externally. There is a function responsible for cyber security.
Very High	*pol_adm*	4	The functions of cyber risk management and oversight are established and play a major role in the decision-making process.

Fig. Contents of knowledge base

The program uses as the knowledge base a *Comma-Separated-Value file*, which contains data about model attributes. A snapshot of the file and its contents is represented in Figure.

A dedicated function has been created that reads throughout the file and extracts the necessary knowledge to be used by the program by filtering the cyber security maturity level, dimension and attributes themselves.

For storing the results of the assessment, the pickle module has been used [3]. This provides and easy method to serialize and de-serialize a *Python* object structure, and will be used for storing the assessment results, as well as reading the previous assessment results. This conceptualizes the data storage for this program. As by module function, the data is stored in byte format. The following code snippets are used to save, and respectively, and load the data from the file:

pickle.dump(indicators, fp)
indicators = pickle.load(fp)

The program uses a main menu structure as a method to improve the usability and fulfill the presentation scope of this program. An existing format for such a menu

has been re-used and adapted for our needs [4]. Upon instantiation of the class, the following code snippet presents the main menu options.

```
def app_menu(self):
    MAIN_MENU = {
      1: {"label": "General Information",
        "func": self.f1},
      ...
      }
```

The concept used here is nested dictionary, which allows to easily read and build a main menu. Respectively, after selecting the main menu option, the respective function is called.

The complete Main Menu has the following format upon program launch:

MAIN MENU
1. General Information
2. Assessment: Policies and administration
3. Assessment: Training and Education
4. Assessment: Work Environment
5. Assessment: Cyber Risk Management
6. Print latest results
7. Exit

The menus are self-explanatory, and we briefly present the main actions that these perform.

The *General Information* option presents the overall cyber security maturity score per each dimension, as well as a performs a brief action to evaluate the maturity level against a set threshold. If the maturity level is below average, which we believe is a high risk, the model warns the user about this fact and encourages for actions to be taken. The output of this menu option by using test data is the following:

Choose a menu option
> 1
***** General information about cyber security maturity level *****
Last assessment performed on: 2021-05-19
Latest average score: 2.9
****WARNING****
Overall cyber security maturity is below average. Actions are required to improve the security stance. To view the results per dimension select PRINT LATEST RESULTS

The next four menu options assess each of the model dimension. The functions first assess the maturity for the selected dimension by looping through all attributes,

and afterwards calculate the average score for the dimension and save the results in the program's database. The code implements this functionality, in addition with other necessary input checks. The output of one step of this function is presented below:

Choose a menu option

> 3

Very High : Comprehensive and regular training programs are established and reviewed based on existing best practices in the field. The training is based on performance and contains evaluations.

High : Regular training programs are established and cover most organizational processes. The training is performance-based and contains evaluations.

Average : Regular training programs are established for all users. These include formal and general issues related to organizational processes.

Low : Training for end-users of the information systems is considered as necessary for only certain technical roles.

Very Low : The training program is formalized to the maximum, often exclusively through reports and recordings without live sessions.

Choose the digit that corresponds to the cyber security maturity level of your organization:

(5-Very High, 4-High, 3-Average, 2-Low, 1-Very Low)

As it can be noted, the program uses the knowledge from the earlier proposed cyber security maturity level. The contents are user readable and easy to understand, and can be adjusted by altering the main knowledge base.

One of the last main menu functions presents the average score per each dimension, as well as calculates and saves a general cyber security maturity score for the organization. The output of this menu implements in our view the ability to identify the dimension that has the lowest maturity. The output of the program, based on given test data for an organization is the following:

Choose a menu option

> 6

Latest assessment results per each dimension are:

-Policies and Administration, last assessment performed on: 2021-05-19, latest average score: 3

-Education and Evaluation, last assessment performed on: 2021-05-19, latest average score: 4

-Work Environment, last assessment performed on: 2021-05-19, latest average score: 1.3

-Cyber Risk Management, last assessment performed on: 2021-05-19, latest average score: 3.2

**** Overall cyber security score is 2.9****

The program developed for the implementation of this model highlights the versatility and options to integrate the model in any risk management system. In addition, it showcases the ability of this model to run as a simple standalone application, that can be used by decision makers in the process of checking the cyber security maturity level, or performing a new assessment. The format and elements used by this program were selected to facilitate the adoption and adaptation of the model by organizations. During development, we have also learned about new options to improve the model, such as by combining the assessment results with various analysis techniques, such as creating a graph of the developments that took place. This, combined with historical data from other organizations, could be useful in selecting the dimensions that logically require actions for improvement. In addition, the model can also be combined with the initially proposed decision support system for cyber risk management, as a main component. In this case, the model can serve as the main code of the system, and in the case where the user decides that risk assessments or treatment have to be made, to used a menu function that would implement the desired function. The interdependence and interoperability of the cyber security maturity assessment model with the decision support systems proves the necessity to evaluate human dimension during the lifecycle of the information system. This application developed as a proof of concept can be used by anyone willing to test the model, as well as support large-scale tests and pilots for assessing cyber security maturity. The code can be refined and adjusted, based on the context, needs and requirements of the implementing organization.

References:

1. BUZDUGAN, A., CAPATANA, Gh. Cyber Security Maturity Model for Critical Infrastructures. In: *20th International Conference on Informatics in Economy (IE 2021)* [accepted for publication], Bucharest, Romania, 2021.
2. BUZDUGAN, A. Model for cyber security maturity assessment in critical infrastructures. În: *Catalogul oficial al salonului "Cadet INOVA"*. ISSN 2501-3157, 6/2021, pp. 154-157.
3. Pickle - Python object serialization: https://docs.python.org/3/library/pickle.html
4. https://github.com/palladog/python-menu-function