Development of a Risk Assessment Model for IT Risk Self-Assessment Expert System for SMEs

Justinas Janulevičius and Antanas Čenys

***Abstract*—The need for a unified Information Technology (IT) risk management methodology is constantly growing due to the increased usage of IT in almost every possible situation. While being a relatively new topic, risk assessment lacks scientific background and unified system to measure the level of risk and compare it to the reference data. While this process requires expertise, results may vary depending on the chosen methodology and the personal experience of the evaluator. Creating a unified risk assessment model is now an initiative supported by governmental bodies worldwide. A risk assessment model for the IT assets that is to be implemented in an expert system is proposed in this paper as well as primary test results of this system are provided.**

***Index Terms*—Risk assessment, expert systems, risk modelling.**

I. Introduction

The increasing usage of Information Technologies (IT) in most of the activity areas brings efficiency, optimization and cost reduction by simplifying routine tasks required by the field of activity. Nevertheless, the beneficial features come along with a wide range of new problems to be dealt with on the daily basis that, if not treated properly, may bring more harm than the benefit of using the IT. Corporate business possesses enough resources to ensure proper IT risk management, while smaller companies, falling into the Small and Medium Enterprise (SME) category are struggling with this issue due to lack of the same resources. This issue of accessibility to the risk management tools is a common reason for failing of the IT assets of the SME Company and therefore causing undesired negative effects.

A risk assessment expert system comes as a solution to the problems mentioned above. It would bring the features of accessibility, instant answering and multi-perspective expertise of risk assessment to the end user, which in this case is an SME company. However, risk assessment, especially in a sensitive field such as IT, requires the expertise to be based on a certain model that would ensure minimal uncertainty with as much factors as possible taken into account. The goal of this study is to develop a risk assessment model for IT risk self-assessment expert system to fit the needs of the SME.

II. Overview of Related Works

There are a number of methods developed worldwide for the risk assessment and management of the SMEs. Some of them, such as Ebios [1], Octave [2] and IT-Grundschutz [3] are available free of charge and offer full support for the needs of the SMEs. Others, such as Mehari [4] and international standards ISO 13335-2 and ISO 17799 come as non-free methodologies for the risk assessment. A review of existing methodologies with provided application fields and examples is provided in [5].

A very strong basis for such expert system is presented in [6]. This attempt presents a Hybrid Intelligent Decision Support System using the risk analysis of European Monetary Union. It also utilizes the Dempster-Shafer theory, enabling to model the reasoning on a fuzzified belief system instead of uncertainty and ignorance. Such factors have led to multivalued approach to belief based reasoning.

Risk measurement as a quantitative size is offered in FAIR methodology [7]. It also provides a full framework for this process that can be implemented in risk assessment to measure different metrics of risk, threat and asset value.

III. Information Risk Assessment

There are three main categories of threats that the information is facing: confidentiality, integrity and availability [5]. The process of risk management enables the control of such risks. It includes identification of assets, threats, vulnerabilities, threat probabilities and damage volume. Given this data it is possible to measure risk that is considered as threat probability multiplied by the damage volume. Knowing the risk allows optimal application of mitigation means.

In this context, threat is considered to be any danger given asset is facing with possible harm. Such threats can either be of intentional or accidental nature. Technical documentation usually describes threat as "a potential cause of an incident that may result in harm of system and organization [8]".

Information risk assessment is a complex multi-perspective process of evaluating possible cases of damages, requiring expertise and lacking formal documentation. It is the first step in risk management process. It consists of definition of quantity and quality values for each situation and identified threat. Risk assessment process follows a certain pattern consisting of threat identification, threat probability identification, assets sensitivity determination, extraction of critical values and controls. Although patterns for risk assessment exist, this process is very sensitive and must be adjusted to every individual situation. This reinforces the idea of IT risk assessment as a process requiring expertise and expert knowledge. While the pattern of this process can be easily described in a formal manner upon a certain

Manuscript received February 1, 2014; revised April 3, 2014.

The authors are with the Vilnius Gediminas Technical University, Dept. of Information Systems, Sauletekio al. 11, Vilnius, LT-10223, Lithuania (e-mail: justinas.janulevicius@vgtu.lt, antanas.cenys@vgtu.lt).

methodology and expertise, it gives an assumption for usage of intelligent computer agents to perform this process. A system of intelligent computer agents forms an intelligent autonomous reasoning expert system fully compatible of taking over all the processes in risk assessment.

In this case risk assessment consists of the following main parts:

1) Threat identification;
2) Assessment of critical asset vulnerability;
3) Risk determination;
4) Risk mitigation means.

Identification of threats the asset is facing is a complicated part due to the variety of possible origins of threats. These include human error, fraud, external and internal attacks, process flaws, problems in governance and management, technical failures, etc. Naturally, the threat list of a particular situation is unique and consists of threats relevant to the activities and assets the subject has in possession. Factors, having the biggest influence on the threat list include the size of an enterprise, the field of industry it is operating in, number of employees, geographical and political situation, internal management and governance. While tailoring the list for specific needs it is important to use comprehensive references as the basis, due to the variety of threats and their sources, and therefore due to high level of uncertainty. Combining general concepts, provided by the standards and regulations combining them with threat activity trends provided in periodical technical documentation [9] gives the most precise output with the most threats covered.

Since the threat is relevant on many factors, the next step is to assess the vulnerability of critical assets by a specific threat. In this stage it is important to determine what possible damage can be done in case the threat occurs. It is worth mentioning that although an asset can be the same, in two different situation the vulnerability may be different according to the value the asset has for the specific business. As an example, a Denial-of-Service attack on web-page based business has a much higher impact than the one working on local retail business and using the web site for advertising purpose only.

Once the threat list and the vulnerability is complete, risk determination is performed. Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. A simplified description of risk provided in Computer and Information Security Handbook shows that the three components of risk are threat, vulnerability and asset value: Risk=Threat × Vulnerability × Asset Value [9]. To measure the risk, the two critical dimensions are impact and likelihood of occurrence. So a simplified expression of the previous statement enables the measurement of risk. To measure the risk certain intervals of the magnitude are assigned to a desired amount of values. In this case the magnitude is to be expressed as INSIGNIFICANT, MINOR, MODERATE and SEVERE. The likelihood of occurrence is then categorized into RARE, UNLIKELY, POSSIBLE, LIKELY and VERY LIKELY. The risk is measured by the interaction of likelihood and impact. A simplified example of risk measurement is shown in Fig. 1. In this case we have defined 5 levels of risk: VL – very low, L – low, M – medium, H – high, VH – very high (critical). Depending on risk level from such model, data, necessary for risk assessment is collected for mitigation controls. The highest risk threats are a priority to mitigate, therefore any threats that fall in the VH category are the most important to eliminate or mitigate. On the other side, threats that fall in the VL category might cost more to eliminate than to let them occur. Therefore, optimum amount of effort has to be put in threat elimination or mitigation depending on the risk it makes the asset face.

While IT risk assessment is a relatively new topic, there is still a lack of formalization of the topic. Risk assessment is a process of measurement, leading to effective management with optimal amount of effort to ensure effective management and safety. Finding the optimal solution requires correct measurement [8].

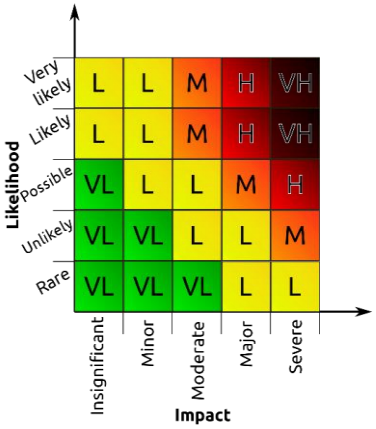

Fig. 1. Risk evaluation map through likelihood of threat occurrence and the impact.

IV. Development of a Risk Assessment Model for the Expert System

While there is a goal of a functioning automated risk assessment tool based on expert systems, it requires a model to be based on. Such model has to meet certain requirements and ensure that the processes are easy enough to understand for a non-professional user as well as getting the most information for the assessment. It is intended that most of the information would be acquired through a Boolean type answers (Yes/No).

In this case the model must ensure these critical parts are covered:

1) Determination of organization capability of performing risk self-assessment;
2) Determination of the business dependency on the IT;
3) Identification of the assets;
4) Identification of threats and vulnerabilities;
5) Identification of existing mitigation means;
6) Identification of current amount of risk along with further risk management solutions.

Determination of organization capability of performing risk self-assessment is based upon the resources available to successfully accomplish such task. The main aspect of this part is to define if the complexity of the IT infrastructure matches the resources, required to accomplish this part. It requires the ability to understand the infrastructure underlying the business processes.

If the first part turns out to be plausible, determination of the business dependency on the IT deals with further investigation of the company. While the company may have the same assets, the impact of their failure might be significantly different depending on the area of business and the criticality of such component.

Asset identification is one of the most important processes in risk assessment. The main goal here is to point out and prioritize the assets that have critical value to the processes of business. Such assets may fall into such categories: systems, network, human resources and applications [10].

Threats and vulnerabilities are then identified depending on the asset list. Their impact on confidentiality, integrity and availability is analyzed. This aspect is very important for correctness of the risk assessment, since the magnitude of the impact for the same asset can differ due to business dependability on it. Therefore such model must ensure different impact values for different fields of industry. In this case the model has several scenarios, chosen depending on the activity of business the company is into. These scenarios define the impact magnitude by processing initial company data, and extracting certain features that describe business dependability on IT [11]. Since the system is designed to perform as an aid to meet regulatory requirements, these levels are provided:

1) No dependency on IT – Business does not incorporate any kind of IT solutions at any stage and therefore does not require further risk assessment. This scenario has very low possibility, yet some small businesses, especially in developing countries, tend to avoid IT solutions due to lack of initial investments or minimal technological expertise.
2) Low dependency on IT – Such business uses basic IT solutions, yet malfunctions do not stop the overall process of the business. Therefore, such business is able to ensure relatively smooth processes with only minor inconveniences. This category is typically a small business, providing non-IT related services and usually dealing with a narrow-spread geography. Therefore IT is used as a convenient communication method and/or minor self-advertising mean.
3) Medium dependency on IT – Business with a sophisticated IT infrastructure, that relies heavily on the IT. Such business uses enterprise resource management and/or customer relation management along with geographically widespread communication solutions. Failure of IT would have a major impact on business processes and cause major damage.
4) High dependency on IT – Business is in the IT field, therefore any malfunction of the IT has a critical effect on the business processes. Failing IT components can cause complete shutdown of business processes and reliability of the company. Such business is extremely aware of fluent, incident-free IT environment. While such kind of business usually has professional risk assessment and management resources, this model is useful for self-control checks of company's internal risk management strategies.

Based on the scenario that the profile of the company falls into, there is an impact volume ratio matrix that provides risk evaluation corrections depending on the scenario. This process allows proper identification of the impact magnitude and therefore corrects the risk and management recommendations.

To avoid excess preventive actions that can lead to overspending on non-effective solutions, the assessment process requires providing the existing mitigation means that are taken into account. Certain controls for the residue risk are then offered to minimize the risks. The optimum risk management strategy, however, does not ensure full prevention from threat occurrence but offers a solution with minimal risk while the costs for implementing controls do not exceed the magnitude of possible damage.

Most parts of this model are realized in a yes/no question way, so that it is easy to understand by the user. For example: to define if the organization is applicable for risk self-assessment, the system requires answers to questions: *Does the company have IT asset list, is there anyone in the company familiar with the IT infrastructure and business processes, is the IT infrastructure critical to business processes.*

V. Model Realization

To ensure the proper functioning of proposed model a proof-of-concept is carried out. The requirements are:

1) Precision – the risk assessment process carried out by the system has to be precise and ensure high quality of output results;
2) Easy to understand – the front-end users of this model are non-professionals in IT, so the interaction between the user and the system has to be simple;
3) Prompt results – the model has to ensure that the results are provided promptly;
4) Compatibility with technical documentation – IT governance compatibility is essential in order to ensure the legislative issues are taken into account;
5) Compatibility with expert systems – this model is to be implemented into an expert system, therefore it has to ensure proper data input and output when realized;
6) Technical part of realization ensuring accessibility, stability and compatibility with modern technologies.

To meet these requirements a platform with web support and wide-spread popularity has to be chosen. Moreover it has to be compatible with complex architectures, operating in both client computer and server.

In this case the server part along with the inference engine has been developed under Java architecture to control and arrange all the processes on the server side. It gives the ability to control the process from client computer while the main operations are performed on the server side. Inference and expertise generation is developed using a specialized Java Expert System Shell (JESS) that is capable of rule generating as well as reasoning. To allow the system to perform reasoning under Fuzzy-logic, an additional library, the FuzzyJ is used.

The compatibility between Java and JESS enables optimal usage of these two components when needed. In this case JESS operates the knowledge base, consisting of rules needed

for the assessment, as well as reasoning while the main application and the interface is written in Java.

VI. Conclusions

The new expert system, dealing with SME risk self-assessment requires a simplified approach to the acquisition of needed information for risk assessment. That ensures higher accessibility by broader amount of non-specialists in need to deal with risk assessment of the business. Since the main aim of the model is to ensure the non-specialist usage, it uses a simplified approach of information acquisition from the user.

General description of the model, used in the expert system is presented in this paper, as well as introduction to realization of this model.

The expert system shows great perspectives in mass risk assessment, however, dealing with collected information and the weights of certain factors requires further investigation.

References

[1] *Expression of Needs and Identification of Security Objectives*. *EBIOS Method of Risk Management*, French National Agency of Information System Security, Paris, France, 2010, pp. 8-19.

[2] C. Alberts, *Introduction to the OCTAVE Approach*, 1st ed. Pittsburg, USA: Carnegie Mellon Software Engineering Institute, 2003, ch. 2-3, pp. 3-12.

[3] *IT Basic Protection, Methodology*, BSI standard 100-2:2008.

[4] *Mehari. Risk Analysis and Treatment Guide*, French Club of Information Security, Paris, France, 2010, pp. 4-18.

[5] J. Vacca, *Computer and Information Security Handbook*, Amsterdam, Netherlands: Elsevier, 2009, pp. 259-267.

[6] A. L. S. Gordon, I. Belik, and S. Rahimi, "A hybrid expert system for IT security risk assessment," in *Proc. Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA '10)*, 2010, pp. 430-434.

[7] J. Clarke, *Consumerization of IT: Risk Mitigation Strategies*, Heraklion, Greece: European Network and Information Security Agency, 2012, ch. 4, pp. 6-15.

[8] *Information Technology – Security Techniques – Information Security Risk Management*, ISO/IEC standard 27005:2008.

[9] J. Jones, *An Introduction to Factor Analysis of Information Risk*, Spokane, USA: RMI, 2005, ch. 7, pp. 34-44.

[10] *Risk Management Guide for Information Technology Systems*, NIST standard SP 800-30 Rev. 1.

[11] G. Patsis, *Information Package for SMEs. ENISA Deliverable*, Heraklion, Greece: European Network and Information Security Agency, 2007, ch. 5, pp. 27-43.

Justinas Janulevicius is a PhD student at the Department of Information Systems, Vilnius Gediminas Technical University.

His research interests are information security, expert systems, knowledge engineering and technical diagnostics.

Mr. Janulevicius is a member of Technical Diagnostics Technical Committee of International Metrology Confederation IMEKO.

Antanas Cenys is a professor at Vilnius Gediminas Technical University.

His research interests are network security, cryptography, nonlinear dynamics in information technologies and electronic systems, nonlinear time series analysis in physics and biology.