RISK MANAGEMENT IN THE ELECTRONIC BUSINESS

Prof. Georgeta Soava Ph. D
University of Craiova
Faculty of Economics and Business Administration
Economics
Craiova, Romania
Ec. Mircea Raduteanu Ph. D
University of Craiova

Abstract: : Risk should not be understood as a destructive phenomenon, but bear in mind that managers who know how to use it can lead to real opportunities. Manager must first recognize the existence of risk, namely to identify and then use specific methods to avoid or reduce the risk. The purpose of this paper is to enter the world, at all simple, of risk management, relatively easy concept to understand but not so easy to put into practice. Of course, the approach relates primarily at the risks inherent of the business in digital environments, but they not represent only a particular case of the risks they are exposed, in general, the companies. In the paper we put in evidence the significance in general business, risks in e-business, then we added a description of the types of security risks, an exemplification of these and a series of test scenarios, and finally to make a analysis of operational solutions of risk management.

JEL classification: L21, C88, D81

Key words: risk; e-business; management; security; applications

1. INTRODUCTION

In a modern society in which globalization manifests it strongly, which imposes a permanent transformation of the business environment, it is necessary to continuously adapt to the needs of business customers. Needs have increasingly grown for ensuring flexibility, rapid response to actual market conditions, fierce competition locally and globally, and continue the process of revamping the purpose of increasing efficiency, have made as the companies to be forced to change their economic model and get involved in electronic business by: reducing distribution channels and selling directly to the customers; use new ways to develop products and services; integration of the value chain with of their business partners.

Thus, the electronics business is founded on the presence of the Internet, which assumes interactivity, namely a permanent connection between the elements that contribute to the achievement of business (producers, consumers and service providers), flexibility, leading to reduced costs, increased quality and efficiency, which manifests itself in increased customer satisfaction.

The business carried out by electronic means, have a certain specific, but not must forget that beyond the prefix 'e', the business is guided by laws valid for any company. The need to anticipate risks and to mitigate possible losses is an axiomatic feature of any

business, in fact constitutes the centerpiece of the "job description" for any manager. In this respect, the manager must first recognize the existence of risk or to identify it, then he use specific methods to avoid or reduce the risk. This paper aims to present business risks inherent in digital media and makes an analysis of operational solutions of risk management.

Perhaps many of those who had leadership positions have made ”risk management” without being aware of this. But is obvious, because every manager has developed a business plan, an optimization of the production process or business, bought an anti-virus or simply respected the rules of labor protection, all these are nothing but reducing, eliminate or at least mitigate of the negative factors that could adversely affect the business, so are risks.

It should be noted however, that no company can predict or cope with absolutely of all possible risks, and without any intention of cynicism, the tragic events that shook the United States September 11, 2001, represent undoubtedly the ultimate argument in support of this idea.

In one form or another every company, from the obscure SRL to large transnational corporations have applied one or other of risk management techniques and thus the paper presents some aspects regarding business risks and risk management stages.

Electronic Business is not newly emerging, but their development is growing, constantly appearing new areas and business ideas that can develop in the online environment, which caused me to address in the e-business risk. We present some examples of business security risks, we have defined the concept of e-business risk management and we presented some risk management technologies at the company level.

2. GENERAL ASPECTS OF BUSINESS RISKS

Identify, isolate and minimize risk requires a careful analysis of the processes or phenomena, which often is subjective, therefore the results are negative. Complete elimination of risk is quite difficult; there is always a balance between the money - risks, so high risk can be reduced by an amount of money directly correlated with its size. Another alternative, which does not use a large amount of money to compensate for the high risk exposure, consists in the analysis process or phenomenon to the point where there is the possibility of finding a balance in the risk - money ratio, the balance in which the risk uncovered can be turned into an opportunity for a new business or lines of current business development.

Risk is a measure of the inconsistency between the different possible results in unfavorable or less favorable conditions. Beyond the purely philosophical aspects of this assertion, in the business world, the inherent risks at which a company is a complex matter, difficult to assess or predict (Terry, C., Webb, M., Griffith, M., 2001).

It is said today that a company is all the more performance with how manages to find more efficient solutions to eliminate the risks to which it is exposed. In ideal conditions, hypothetical, without exposure at risk, a company would produce maximum profit associated with its production capacity with the condition to be alone on the market. How this is not possible in real life, by the appearance of a competitor suddenly appear dozens of other risks to which both companies are exposed.

3. THE PROCESS OF THE RISK MANAGEMENT

The present study is based on the secondary data. In this regards, Neuman’s (1997) document analysis is very useful for systematic analysis of a particular topic. Therefore,

data were collected from published and unpublished materials, books, newspapers and ongoing academic working papers.

Risk management is defined as "uncertain event management in order to achieve success." Its main feature is the uncertainty as major base of the risk factors, thus is necessary the selection and use of appropriate methods and means of the risk management.

According to Opran (Risk management, 2013, pp.18), risk management must be "systematic" because he believes that to achieve effective control over activities managed and reduce risk factors requires a rigorous approach, constant and thorough at all levels of business development. Thus, we can say that risk management activities involve the use of information from different areas (economic, legal, technical, political, psycho-social).

Risk management involves an risks assessment (identification of risk factors), a program of response to risk factors (finding an appropriate response strategies for each risk separately, depending on the type and degree of seriousness), monitoring and controlling risks (implementation of response strategies and monitoring the effects that these can bring, adjusting them according to the effects they produce) (Opran, C., Risk management, 2013, pp.20).

4. ELECTRONIC BUSINESS RISKS

Revolution "e" had a positive effect on business developed by the Internet and beyond, streamlining payment flows of production, customer relations, etc. In this context, the Internet plays a major player by connecting companies with customers, or its suppliers worldwide.

To be competitive in the newly created business world, companies must develop strategies that focus on response time to market demands and customer service. Customers should have more choice in the new (e) economy. If to a company it takes a few months to provide a service and the competition does this in a few days, it is clear that the first company will go bankrupt. Companies need to transform their own internal systems, to be noted that the transition of the traditional business to e-business, however, is associated with an increased number of risks. Thus, when conducting business via the Internet, there are a number of risks related to the information veracity from the network, and of the access of unwanted people in the system.

One of the most common sources of risk is the security and inadequate control elements within enterprise resource management systems (ERP). Beyond internal organizational chaos that may occur in the case of companies with a Web component, usually, these systems are directly related to the management of relationships with customers and suppliers, or even with the Web sites, case in which exposure risk is exponential.

Potentially dangerous situations can arise and in violation of the regulations or contracts with serious legal consequences, ranging from pay harsh fines or penalties, to criminal offenses. Another risky situation is the one where business processes are inoperable or missing. Crisis highly publicized dot-com sites, that have failed massive and such is an implacable argument. Simple building a website, behind which there is no production or distribution system has made as many dot-com sites to wake up face in face with nothingness. A risk factor is represented by cases where simply there is not sufficient knowledge for making decisions or the investigations launch. It derives directly from inadequate capabilities of IT risk monitoring.

A frequently encountered situation is when unmanaged changes occur in IT infrastructure of companies. Installing software or hardware may, in case of faulty configuration voluntary or not, to produce security holes in the company's IT infrastructure, which leaves the way open for another range of risks represented by the unauthorized access of the systems. Such unauthorized accesses occur mainly within the organization, representing the internal factors, but can also be external factors such as infestation of the systems (viruses, worms, Trojan horses).

Risks can also be of a structural nature in organizations where were put in place policies or ineffective security infrastructures. Also important is the escalating IT costs, that make as budgets simply do not reach at implementation of anti-risk effective policies, common thing unfortunately in Romania. Poor quality of services offered by a company can push potential customers toward the competing sites, with direct effect on revenue, which can block the whole business process.

Beyond the claim to find recipes or identical patterns applicable, can be defined the main categories of IT risks which permanently pressing of the companies.

Potential risks that I wanted to address them are related to IT security, of that a company has or intends to implement them. It is important to note, that the danger can come from both internal users and external stakeholders, while seeking to "break the code" to enter into the computer system. Generally, the risks of the Internet activities increase whenever access is granted to persons outside the company network.

Although companies have started to reorganize the way to do business, and rely increasingly on electronic business, they are not prepared for ensuring electronic security, and this can cause losses both financially and especially the company's reputation.

In the electronics business, the risk management involves: assessing risk, developing the damage control, the systems compatibility and elaboration of a response plan in case of emergency.

It is clear that frauds could occur most frequently in the least risky areas and weak protected, which can provide significant gains. If effective protection is achieved, we will see a minimization of illegal entry and its absence will not only allow penetration system but can increase the number of incidents. The method by which companies can protect their documents is encryption their.

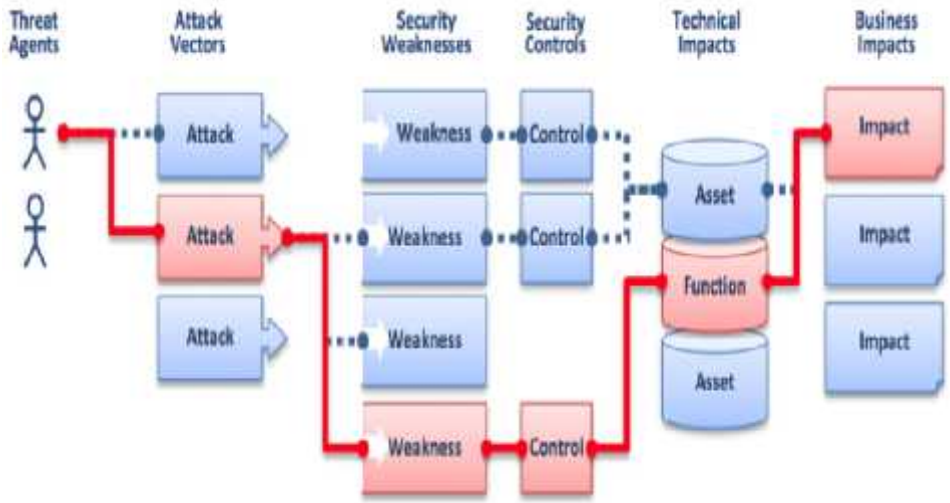
Another type of risk with that companies may face is the "attack-sites", which are a collection of dissatisfaction and complaints received from the customers against poor services offered by different companies. There may however be cases where these complaints are sent even their own employees or competitors in an attempt to discredit the company. The methods by which a company it can defend of such attacks consist in registration of the companies sites name which doing negative publicity and of the pirate firms (by changing the extension).

A company can be competitive if you perform a system evaluation, an insurance of the protection and the establishment of action scenarios (Mihăescu L, 2009, pp.128).

5. RISKS RELATED TO BUSINESS SECURITY

Risk is generally defined as a combination of the probability of an event and its consequence (ISO Guide 73). IT risk can be defined as a potential threat that're mining IT system vulnerabilities and thus may harm the organization (ISO / IEC 27005 FDIS: 2011). According to CNSS Instruction No. 4009 (2010) risk is the possibility that a certain threat to have a negative impact due to exploitation of the computer system vulnerability. IT-related risks defined as probabilities of occurrence of certain threats can be triggered

accidentally or intentionally will print a specific vulnerability of the information system what may result in some loss. IT risks always exist, regardless of whether or not detected or recognized by the company (figure 1).



Source: What Are Application Security Risks?, https://www.owasp.org/index.php /Top_10_2013-Risk

Figure no. 1 Risk Management Process Application Security Risks

Any attacker can use several ways to affect the organization or business. Each path can be a risk that can be treated, depending on how important it is. Although these paths can sometimes seem trivial, for to find them and exploit them sometimes proves to be extremely difficult. To determine the risk must be assessed the probability associated with each threat agent, attack vector, or weakness in security, then analyzed and estimated the impact on the organization. The most common risks are:

Injections. Risks regarding SQL injections, OS or LDAP, occur when unreliable data are sent to be interpreted as part of an order or instruction. Invalid data sent by the attacker can trick the interpreter to execute unauthorized commands or to access private data.

Cross Site Scripts. XSS weaknesses occur when an application uses unreliable data, on that it sends to a web browser without proper validation. XSS enable attackers to conduct scripts in the victim's browser; these scripts can hijack user session, website deformed or redirects the user to websites ghost (Web Security Cheatsheet / ToDo list, 2013).

Examples of test scenarios

1. Scanner Acunetix XSS. When starting the scenario, the test is configured with the desired parameters and with profile you want search, in this case, XSS. A possible response of the test looks like as figure 2.

2. Using the manual insertion of scripts in various parts of the application. This method is used not only to check the results with Acunetix for accuracy but to be sure that all vulnerable files are checked.

Incorrect authentication and session management. Application functions in terms of authentication and session management are often implemented incorrectly, thus enable remote hackers to compromising the passwords, keys, session tokens, or force other weaknesses of implement to get other user ID in the application.

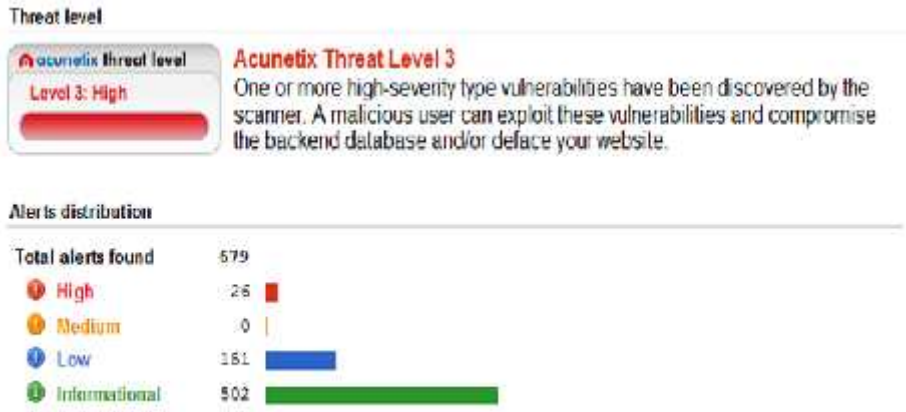


Figure no. 2 Response of the test

Unreliable references to objects. This will enable the hacker to break the victim's browser and generate the requests in that vulnerable application interprets them as legitimate (Web Application Software Security, 2014).

False requests in Cross Site. A CSRF attack forces an authenticated victim's browser to send fake HTTP request, including the victim's cookie session and any authentication information by a vulnerable application. This allows the attacker to force the victim's browser to generate requests in that vulnerable application interprets them as legitimate.

Examples of test scenarios

1. Using Acunetix CSRFscan. When starting the script, test parameters are configured with the desired profile you want and search, in this case, CSRF. A possible answer to the Acunetix might look like as figure 3:

Figure no. 3 Response of the Acunetix

2. Using the manual scripts in different parts of the application. Different scripts can be used in applications to test this risk. All checks should be made by users logged into the application of various types, because the risk exploits user rights in the application. The following scripts can be used to simulate an attacker who is trying to add dangerous code in website: (1) HTML Methods: IMG SRC: <img src=”http://host/?command”>, Script SCR: <script src=”http://host/?command”>, IFRAME SRC: <iframe src=”http://host/?command”>; (2) JavaScript Methods: ‘Image’ Object (<script> var foo

= new Image (); foo.src = “http://host/?command”; </script>), ‘XMLHTTP’ Object on IE (<script> var post_data = ‘name=value’; var xmlhttp=new ActiveXObject (“Microsoft.XMLHTTP”); xmlhttp.open(“POST”, ‘http://url/path/file.ext’, true); xmlhttp.onreadystatechange = function () { if (xmlhttp.readyState == 4) { alert(xmlhttp. responseText); } }; xmlhttp.send(post_data); </script>).

Security misconfigured. A good security involves to having a secure configuration, defined and put into practice for the application, frameworks, application, web and database server, and platform. The settings will have to be defined, implemented and maintained because many of them have predefined settings. This means regularly software updating, including and code libraries used by the application.

Uncertain protect of data. A lot of the web applications, do not adequately protect the confidential data, as credit cards example, login data using appropriate encryption or a good hashing mechanism. Attackers may steal or modify unprotected data to steal identities, to credit card fraud or other illegalities.

Unauthorized access of URLs. A lot of the web applications verify the URL access rights, before executing / loading of protected links or buttons. These applications should also execute these checks every time pages like this are run, otherwise attackers can forge URLs to access these hidden pages.

Network insufficient protection. Applications always fail to authenticate, encrypt and protect traffic confidentiality and integrity with sensitive data by network. And when they do, use weak algorithms, expired or invalid certificates, or does not use correct the safety procedures.

Invalidated redirects. Many times, the web applications, redirecting users to another pages and websites and using unreliable data to determine the destination pages. Without a corresponding validation, hackers are able to redirect victims to unreliable sites (with viruses or dealing with the deceivers), or by the unauthorized pages (with viruses or dealing with the deceivers), or by unauthorized pages.

DoS attacks. A DoS attack is an attempt to make a computer or unavailable network to users. Although the reasons, way for achieving and the target may be different, the attack assumes in generally the concerted efforts of a person or many persons to prevent a web site or service to function efficiently or at all, temporarily or permanently.

More applications can be used to test this potential vulnerability as: (1) Udp.pl Which is a UDP flooder application written in Perl; (2) Sarpe.pl is a Perl script that sends TCP without flags and compel victim to respond with RST packets. It seems to be more efficient than a SYN attack and harder to detect; (3) HTTPerf is an application that measures the performance of a web server; (4) Charles Proxy HTTP year proxy / HTTP monitor / Reverse Proxy that provides the ability to see all HTTP traffic and SSL / HTTPS between machine and internet.

Data manipulation. Most attacks to web applications involve requesting a website with manually enter data to generate an unexpected context. The HTTP protocol enables transmission parameters requests and can do this in several ways: Cookies, Field's on forms, URLs, HTTP Headers.

It is crucial to understand that these methods of data transmission can be easily manipulated by a user, and therefore, it is preferable to consider as a user is not reliable. Thus, the security can not be based solely upon checking on the client (values proposed by a HTML or checked with Javascript).

These tests can be done in several ways depending on the specific application and how it is developed:

1. Change Ids. This scenario can be tested using the Chrome browser with the integrated tools for development or Firefox with add-on Firebug. For this, on a certain page where it edit an article, must searched using one of the options above, a hidden input where ID is saved. If this field exists, the user could change the ID and save the article, so it could prejudicial information from the database.

2. Inserting of values into a input with fixed values. Similar to the scenario from section 1, a dropdown is selected and the values are modified, and then saved. Importantly, its can not be saved in the database corrupted data.

Waiver of privileges is the action of exploiting a fault of system, design or a configuration mistake to get access to resources that are normally protected by an application or a user. This vulnerability leads, for example, to access information or the account to another user.

Identity falsifying. In the context of network security, of falsification attack is a situation in which a person or a program manages to impersonate someone else by falsifying data and have illegitimately gain access. Many TCP / IP protocols fail to provide mechanisms for authenticating the source or destination of the message. In this way, they become vulnerable to of falsification attacks when extra precautions are not taken to verify the identity of the host application that sends or receives.

Examples of test scenarios

1. Checking the sensitive information/useful that could be used. This can be done by checking the data stored in the page source "ViewState" and tested using Fiddler 2 and ASP.NET ViewState Helper. It Opens Fiddler application along with IE. The user navigates to a particular page and opens the ViewState Inspector. All requests are displayed in the test application. The user selects a page and sees the information "ViewState" decoded.

2. Using Base64 online decoding programs. "ViewState" information is copied and decoded using Base64 online decoding programs. This scenario can be executed to validate or invalidate the results from Scenario 1.

Shell injections known as command injections, are not most commonly discovered vulnerabilities but are some of the most critical. Very often the web applications need to use other programs or applications to perform certain functions. This may involve a simple scenario such as sending an e-mail using a UNIX program or something more complicated: the execution of perl or c ++ custom programs and orders. If the data is sent to the user interface programs, then the attacker can add shell commands in these programs and can thus compromise good execution or the system.

Injections with files. This attack is used to exploit the "dynamic tabs include" mechanism in Web applications. When web applications use user input (URL, parameters values, etc.) and places them into commands for inclusion of files, the web application can be tricked into include files containing dangerous code. Such an attack allows the attacker to: running dangerous code on the server, which could lead to compromising the full system; running dangerous code on client systems. The attacker can add code that will be executed in response to client (e.g. Javascript code to steal session cookies from the client).

Examples of test scenarios:

1. Using Acunetix scanner for SQL injection. Acunetix Scanner for SQL injection has the Blind SQL Injection option.

2. Using the manual scripts that include specific characters. Various tests can be done by trying to insert scripts in various input or URL application.

Hidden content encryption. In cryptography, encryption is the process of transformation of the data using an algorithm to protect it of those who do not have the decryption key. Unencrypted information by users can be exploited by hackers to steal in some cases vital information such as credit accounts.

6. eBUSINESS RISK MANAGEMENT

Risk Management effectively allows an increase in business performance in achieving the strategic objectives of the enterprise through efficient correlation between information and the technology risk.

The activity of any enterprise risk management involves a complex tool of assessment that allows identification of risk factors, prevention the activity interruptions, avoid the security vulnerabilities. Addressing these investigations both from the perspective of internal and external, leads in terms of information systems on identify of the security risks to physical, logical, application and data level and mitigate or correct them before being used in illegal purposes.

Specialists propose to achieve these goals a number of steps, and the first step is to identify and understand the nature of the risks, and defining risk tolerance of the company, i.e. the maximum level to which possible losses without compromising business objectives. Once established these things are then sought methods and measurement systems as accurately risks and ways to their monitor. The next stage is putting under control of the uncertainties related to the smooth running of the business, leading finally to understand the impact that may its have the risks of the catastrophic nature on the company. One of the key elements in achieving these steps is elaboration of a risks map, in which each of the identified risks is represented by a coordinate system probability / impact. It will be seen that the points tend to concentrate in certain distributions in the chart, which indicates very eloquently not only the type of risks, but also probability to occur and foreseeable impact which may have.

Another concrete tool for risks analysis is the matrix in which for each of the defined risks, it evaluates the impact the respective business risk, the probability that it would come at some point, the degree to which the company is prepared to cope but and concrete responsibilities broken down by activities type. This array, when completed, is a comprehensive risk management plan, Business Continuity Planning (BCP).

From studies, we can say that in the Romanian business environment, the concept of "risk management" is understood correctly by the majority of senior staff, but effective risk management is not yet a priority for companies in Romania. In this context, non-allocation of funds has been identified as the main reason why this concept is not implemented seriously in Romania (Money.ro, 2013).

7. TECHNOLOGY, ADVANTAGE IN RISK MANAGEMENT

The concept of risk keeps to our inability to know what the future may bring us, as response to a specific action. For companies whose business has fierce competition and the business environment is uncertain, the methods and tools for risk analysis prove to be a very useful ally that can make difference.

In the following we will take a look at one of operational risk management solutions, available on the Romanian market. More specifically, it is a suite of Decision Tools Suite from "Palisade Europe" - that turns ordinary Excel into a powerful tool for risk analysis and support strategic or operational decision. DecisionTools Suite is software produced by Palisade Corporation is able to offer solutions for risk analysis, representing a

robust and innovative decision support. The most recognizable product, @ RISK performs risk analysis, with over 150,000 users in more than 100 countries and is translated into seven languages. RISK that can be learned in a few days is a module that can be added to Microsoft Excel and Microsoft Project, becoming best known in the world to conduct a risk analysis to managerial level (Palisade, 2014).

Building on the success of the module @ RISK, Palisade has developed other programs to meet the growing demand for professional software decision support, making as the DecisionTools Suite, a complete set of tools for quantitative risk analysis in order the most effective decisions, including modules: PrecisionTree, Evolver, @ RISK, @ RISKOptimizer, TopRank, Neural Tools, StatTools. Below we highlight the advantages of package by modules: PrecisionTree, and @ RISK.

Precision Tree is an add-in for Excel that brings advanced concepts of modeling and decision analysis Microsoft Excel work environment, based on the traditional model of decision tree. The decision tree involves consideration of the "operational risk" based on the indeterminacy of the situation and it inability accurate forecasting.

Determination of the optimal solution actually means finding the best way, a most appropriate tree branch from the initial to the final node. The results include a full statistical report and graphical of the risk profiles, offering graphics with possible suggestions or strategies. PrecisionTree analysis includes in achievement of the risk profiling and statistical report, which provides a statistical summary report of the decision analysis, which allows us to be able to make comparisons between the alternatives chosen.

From the study can be noted that the decision tree shows all possible options of decision and random events in a tree structure. It formed from left to right, showing the events and decisions related. The fact that the data are processed in real time, we are able to test any options we want and finally choose the one that meets most of our desires. Effective use of the decision tree method depends of the information update on the process modeling, being quite complicated, as when drawing up the model, it can be estimated entirely the variants decision. In order to avoid major deviations is need to be tree reviewed and in according to the assumptions materialization it is reviewed the reasoning from the decision intermediate nodes. It is important to note that value obtained for the optimal solution is an average value, which can vary depending on the nature of the event, between a maximum and a minimum.

The deficiencies of the decision tree method, start from the lack of information on the dispersion and shape distribution of all possible outcomes and the associated probabilities of these outcomes. It is very important to carry out a full description of a probability distribution, because makers have different reactions and attitudes towards risk, and the shape of the probability distribution allows shaping of an image about the risk associated with each alternative. To try to limit these shortcomings, we present @RISK package that can achieve a probability distribution.

@RISK tool provides an overview of how to perform analysis of decision under risk using Monte Carlo simulation. For example, someone interested by probability that a Web site to succumb to simultaneous attack of several hackers at a time and under certain conditions. In this case, for the analysis certain vulnerabilities of a network, it can applied Monte Carlo simulation for scenarios based not on financial variables but rather on different utterances. The range of probabilities arising from Monte Carlo simulation is likely to be diverse and more accurate than the results of a traditional analysis, as type "the worst - at best" case. By using the tools provided by the module @RISK, managers are able to consider a variety of options. As a result of the different scenarios, we can view the

scenarios report, which allows us to determine which input variables contribute significantly to achieving a goal, and we can generate a series of stress tests. By using such tests, the managers find which is the combination between variables and including the values to which must tend, thus are generating the best results. On the other hand, we know and the combination of variables with their values, on which must avoid, removing them.

8. RISK MANAGEMENT AUTOMATED SYSTEMS

Running a risk management program, using Excel, it is not successful, because may be too long to update spreadsheets and do not have the tools to keep up with the speed of change. Thus the most effective methods are the automated solutions. However, if makes an analysis is found that these solutions were disheartening because many practitioners in the risk theory still trying to help their organizations understand and manage uncertainty without modern tools. Thus, KPMG (2013) recently conducted a survey of about 100 practitioners in risk management. The result is alarming, 64% were entirely dependent on manual processes. Another recent study Deloitte (2013) found that less than 25% of them achieved continuous monitoring of risk, even if the majority believes that the risk volatility will increase in the next year (e.g., the risks will change faster and involves values older). And yet, with an accelerating pace of change, with a massive pressure from regulators to achieve effective risk management, companies continue to rely on manual processes.

In this way, the SAP Business Suite intelligent solutions can radically change the way companies do business, leading to an acceleration of work processes, thus redefining the speed with which companies operate at a simplification of internal interactions, providing a wide range of opportunities for the growth thereof (Ghițulescu, R., 2013).

Business Suite is a comprehensive suite of business solutions enabling flexible business, full integration and collaboration over the Internet. The real-time technologies, combined with the potential of mobile applications to access data and information in real time, reduces the number of business processes and generate new means in order to change radically the markets, allowing leaders to conduct business based on current requirements. Through this platform, analysts are able to process a large volume of data in just a few seconds to make critical decisions focused on ensuring long-term customer needs, which will lead to revenue growth and profitability of a company.

9. CONCLUSIONS

In the market economy, the business environment is characterized by a particular dynamic, because of permanent need to adapting to market changes, it is necessary to take decisions in real time, it be flexible. The idea of "business" implies, in the life of every entrepreneur, the concept of uncertainty and, at best case, on that risk. Whether aimed at segments that belonging to an initial phase of activity (such as business object definition, or establishment of relations with suppliers) or a phase that aimed at the production process or the results that looming in time, the risk is permanent companion of the company existence, unseen enemy and at the same time, the engine many original actions.

At the risks they face any business firm through starting activity it adds and risks of the online environment, if this opts for an electronic market development.

The issue of risk assessment is well known, long studied and the interest result of that enjoyed among specialists is materializes in models, methods and techniques designed to bring some light on the different risk categories.

Businesses once implemented in the electronic environment have encountered various obstacles, from general of the online environment, up to some specific risks to each business in hand. However risk management is also continuously developing and trying to keep up with new risks emerge and to find new solutions and ways to prevent them. The most effective technique of risk management we believe are the automated solutions. Even if at this time the cost is high, it tends to decrease, and then increasingly more companies will implement a smart business package to dependable support in risk management.

REFERENCES

1. Ghițulescu, R. SAP Business Suite pe platforma SAP HANA, 16 Ianuarie 2013 http://www.marketwatch.ro/articol/11812/SAP_lanseaza_noi_aplicatii_SAP_Business_Suite_pe_platforma_SAP_HANA/
2. Mihăsecu, L. Sisteme informaționale și aplicații informatice în administrarea afacerilor, Editura Universității, Lucian Blaga, Sibiu, 2009
3. Opran,C., Paraipan, L., Stan, S. Managementul riscului, Editura comunicare.ro, Bucureşti, 2013, www.comunicare.ro
4. Terry, C., Webb, M., Griffith, M. The Risk Factor. How to Make Risk Management Work for You in Strategic Planning and Enterprise, England, Harrogate: Take That, 2001,
5. CNSS Instruction No. 4009, 2010, http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf
6. Deloitte The value killers revisited A risk management study, 2013, http://www2.deloitte.com/content/dam/Deloitte/br/Documents/audit/ValueKiller.pdf
7. ISO/IEC FIDIS 27005 Information technology — Security techniques — Information security risk management (second edition), 2011, http://www.iso27001security.com/html/27005.html
8. KPMC Expectations of Risk Management, Outpacing Capabilities – It's Time For Action Top Eight Risk Management Imperatives for the C-suite in 2013, https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/risk-management-outpacing-capabilities/Documents/expectations-risk-management-survey.pdf
9. Money.ro Risk Management - singurul proiect din România, pe managementul riscului, 2013, http://www.money.ro/risk-management---singurul-proiect-din-romania--pe-managementul-riscului_1244937.html
10. * * * Palisade, 2014, DecisionTools Suite
11. * * * Managementul riscului, http://www.scrigroup.com/afaceri/MANAGEMENTUL-RISCULUI-Clasific25326.php
12. * * * Web Application Software Security, 2014, http://proactiverisk.blogspot.ro/2014/05/web-application-software-security.html
13. * * * Web Security Cheatsheet / ToDo list, 2013 http://security.stackexchange.com/questions/2985/web-security-cheatsheet-todo-list
14. * * * What Are Application Security Risks?, https://www.owasp.org/index.php/Top_10_2013-Risk