MODELLING REAL-TIME RISK MANAGEMENT SYSTEM

Vladislavs Minkevics[1], Girts Vulfs[2], Jans Slihte[3]

[1]Ministry of Finance, Smilšu 1, Riga LV 1919, Latvia,

[2]Riga Technical University Kaļķu 1, Riga, Latvia

[3]Ministry of Finance, Smilšu 1, Riga LV 1919, Latvia

Vladislavs.Minkevics@fm.gov.lv (Vladislavs Minkevics)

Abstract

This paper addresses modeling real-time risk management system. Risk assessment is a very important decision tool for investments to support business. When it comes to money no business wants to pay for anything that it does not need, that's why risk assessment has it's significance. If organization analyzes risks, it has to employ a very experienced people which may lead to excessive expenses.

To make risk management effective a solution proposed is real-time risk management system that collects alerts and log files from different systems and based on experience, gained from the previous analysis, analyzes risks. To improve overall security, risks must be analyzed at least once a day for an important systems, but as the matter of fact risk management is time and recourse consuming, usually it is done once a year for each information system. An automated real-time risk management system will solve the problem and there will be no unnoticed vulnerabilities.

A proposed solution for real-time risk management is using unified threat management system which provides alerts and log files for analysis and decision making.

If all possible vulnerabilities and threats are put in count, system will be able to make right decisions how to minimize risk very quickly, which will save information systems from threats exploiting vulnerabilities and will save money.

Keywords: Risk, risk management, real-time risk management, effective risk management, neural networks.

Presenting Author's biography

Vladislavs Minkevics. Working in Ministry of Finance of Latvia as a security manager for five years. Studying information technology. At the moment working on dissertation project. A member of ISACA (Information Systems Audit and Control Association). Have a CISA (Certified Information Systems Auditor) recognition.

ISBN 978-3-901608-32-2

1. Introduction

Nowadays risk management becomes an important part of business, because mitigating IT risks is much cheaper than fighting with circumstances caused by a threat. Risk management helps business to be sure that nothing bad – like loosing important data or even a whole business for some period will happen. With IT risk management we may draw parallels with other field like firefighting. Everybody knows that poor wiring, dry highly flammable materials and open fire may cause fire. With simple things like change wiring, prevent open flames, it is possible to minimize risk of fire. The same could be addressed to IT risk management. If business knows that IT risks are being monitored on timely basis, it may be sure nothing bad happens.

2. Problem

To make sure business is getting actual information about possible threats that may exploit vulnerabilities and risks associated with it, IT risk management must be done on real-time basis.

It may be said that there is a direct correlation between the risk assessment cycle and risk level, because the longer the assessment cycle time the more exposed is the organization is to attacks on critical information assets.

Real-time risk management system should answer the main risk management question (what is wrong, and how bad it is) and make a decision or immediately inform responsible authorities if any risk exceeds the predefined value.[1-4]

3. Theoretical aspects

Risk is a function of the consequences (or impact) of an undesirable event and the likelihood of that event occurring. Risk assessment is the process whereby risk relationships are analyzed, and an estimate of the risk of asset compromise is developed. Compromise includes unauthorized disclosure, destruction, removal, modification, or interruption. Options for managing risk include reduction, transfer, avoidance, and acceptance. A risk assessment produces an estimate of the risk to an IT system at a given point in time. It answers the following questions:

- What can go wrong?
- How bad could it be?
- How likely is it to occur? [5]

Risk management is the process of identifying exposure risks, defining controls and requirements to manage risks, and implementing controls in a cost-effective manner. Ideally risk management should answer those questions:

- What is the risk level of each application?
- How can critical vulnerabilities be found and mitigated?
- How do infrastructure changes impact security levels?
- What is the right priority of remediation actions?

Risk assessment is concerned with understanding the effects of adverse events on a decision, plan, or value of an asset: an assessment not of what did happen in the past but of what could happen in the future. If we can understand how adverse events will change the world then we can insure (or hedge) against them by preparing for that "rainy day." This one of the goals of risk management.

From a quantitative perspective, risk assessment requires a mathematical model of the world consisting of several input factors that are related to a measurable output. A natural setting for such a model is in the realm of probability and statistics. If we assume that we know the underlying probability distribution on how events will play out — and the precise relationship of the input factors to the output results - then risk assessment is reduced to estimating the likelihood of these adverse events occurring over a given time horizon.[6]

4. Why information technology real-time risk management system?

Organizations that are taking care of their information systems, usually are taking risk assessment manually, but it has some disadvantages:

- this method of risk assessment requires experts to be very competent;
- it is hard to create one list of vulnerabilities to include needs of all systems;
- the risk assessment is based on subjective thoughts of the members of expert group;
- risk assessment is time-consuming procedure (risk assessment for one information systems may take a day, depending on criticality of information system);
- because it is time consuming, usually risks of information systems are evaluated once a year, which may cause vulnerabilities and threats not to be noticed.

To avoid these disadvantages, risk assessment could be divided into two parts:

- risk assessment using experts;
- risk assessment done by the system.

Automatic system will not replace the skills of an expert, although it can dramatically increase the accuracy and efficiency of the assessment process. Ideally expert work should be combined with reports from real-time risk assessment system. An expert should participate in evaluation of:

- back-up practice and policy;
- the contents of the recovery plan;
- the status of the recovery plan;
- the recovery location;
- general contingency practice, procedure and policy;
- network contingency;

ISBN 978-3-901608-32-2

- application contingency.[7]

Figure 1 shows a direct correlation between the risk assessment cycle time and the possible risk level. The longer the assessment cycle time the more exposed is the organization is to attacks on critical information assets. Therefore, the most straightforward way to reduce risk is by completing the assessment cycle much faster. It will shrink the window of exposure.
By using real-time risk assessment it is possible to shrink exposure to a single day or even an hour.

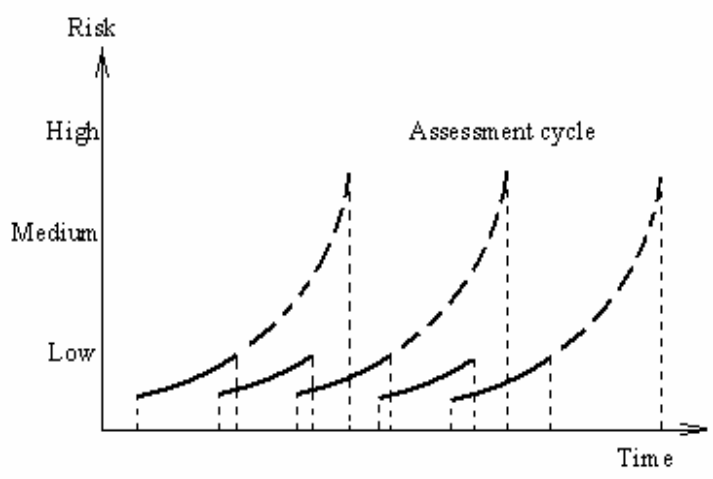

Figure 1 ”Risk assessment cycle”

As most people somehow related to IT security know, only 1-2 percent of all vulnerabilities are truly critical from a potential business impact perspective. The ones that lie along a potential attack path to an important information asset create a real exposure and must be treated as a top remediation priority. In fact, most vulnerabilities are mitigated by specific control mechanisms like firewall or by the network architecture itself.

The security personnel challenge is to identify and mitigate in a cost – effective way critical 1-2 percent of vulnerabilities quickly enough to prevent potential exploitation by attackers. [8]

5. Real-time risk management system

Real-time risk management system’s flowchart is shown on figure 2.

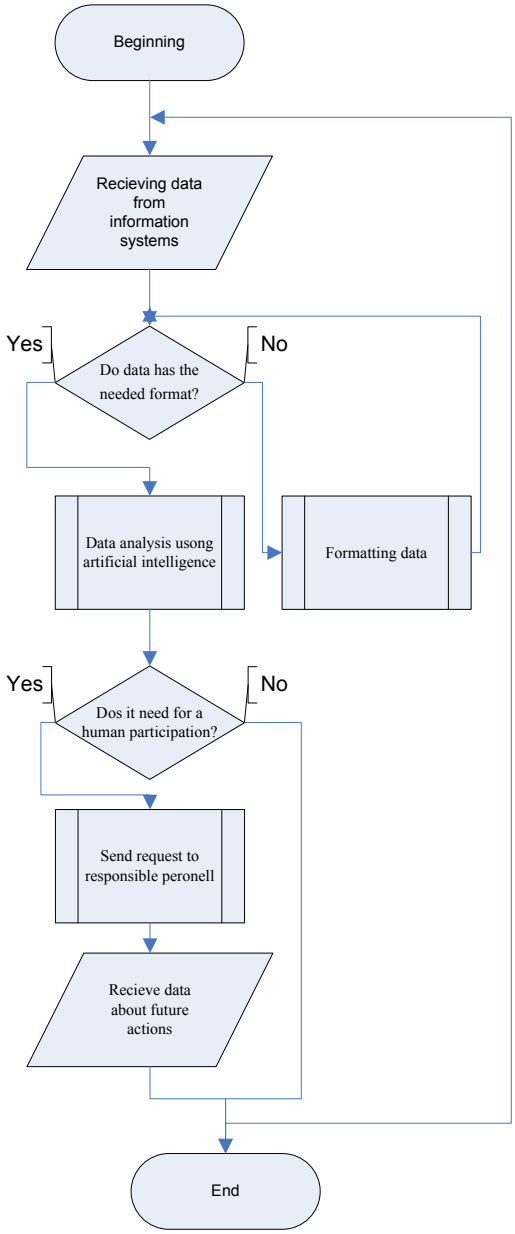

Figure 2 “Real-time risk management system’s flowchart”

To create real-time risk management system which would be able to analyze systems alarms and log files and based on that evaluate risks, there are three main activities required:

1. system should have as much defined risk descriptions as possible;
2. system should have a defined action if there is no such defined risk in systems database, for example it may be able to teach itself;
3. decision should be made according to previously gained knowledge and according to system faults and log files.

Real time risk management system is network based system which is capable to analyze traffic, audit logs, alarms from the systems in network and by using mathematical models, make online risk assessment.

ISBN 978-3-901608-32-2

6. Model of real time risk management system

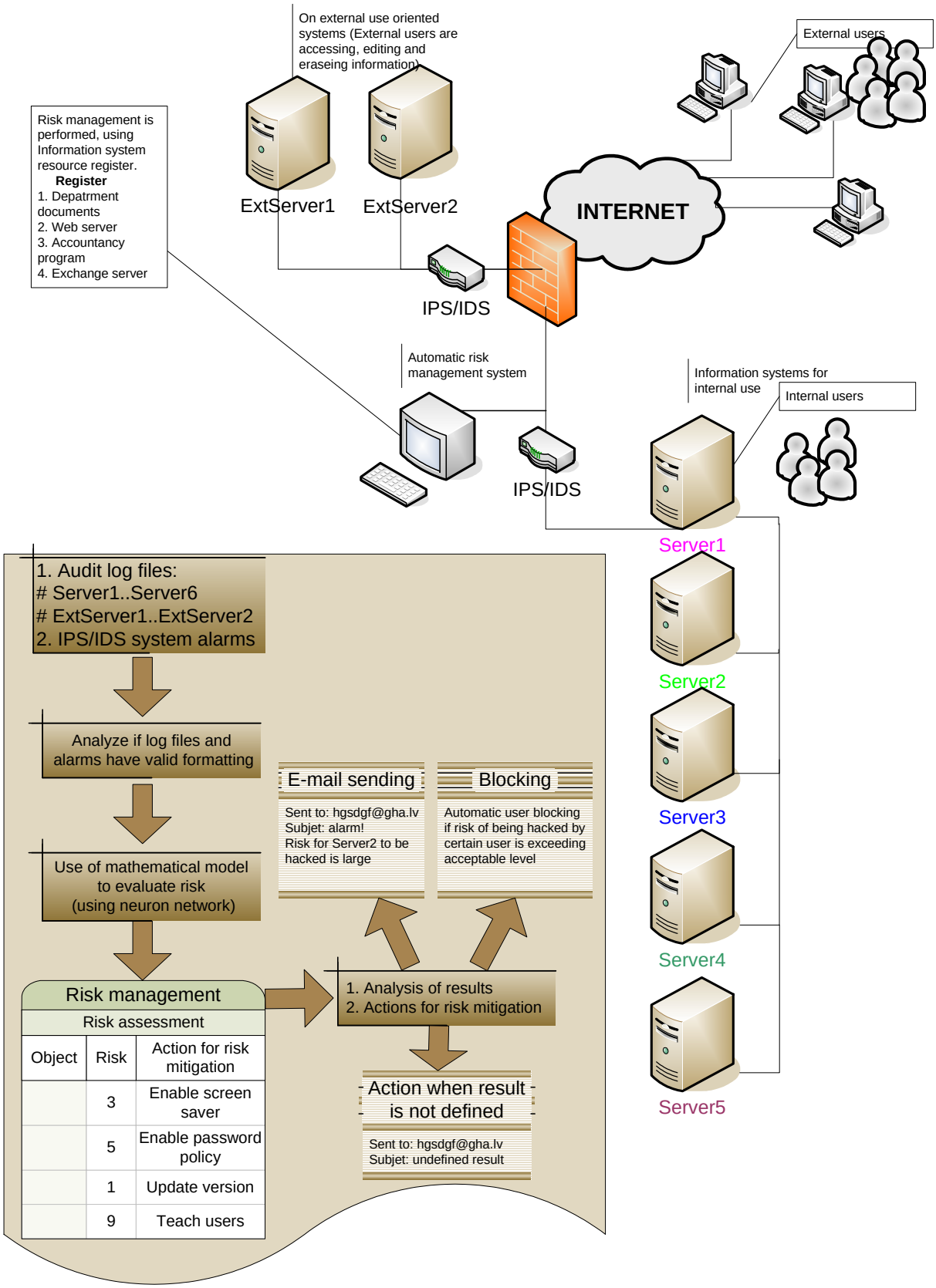

Figure 3 „Model of real-time risk management system"

7. Applying neural networks in model

A neural network is suited for simple to complex, and structured to unstructured problems (figure 2).Thus, a neural networks can solve a much broader range of problems than, for example, expert system, including problems that are almost completely random in nature.
Neural networks can be used to detect trends that are too complex to be noticed by humans or other computer programs, including those depicted in figure 2. A trained neural networks can be thought of as an expert in the category of information it has been given to analyze. This expert can then be used to provide projections given new situations of interest and answer "what if " questions.[9]

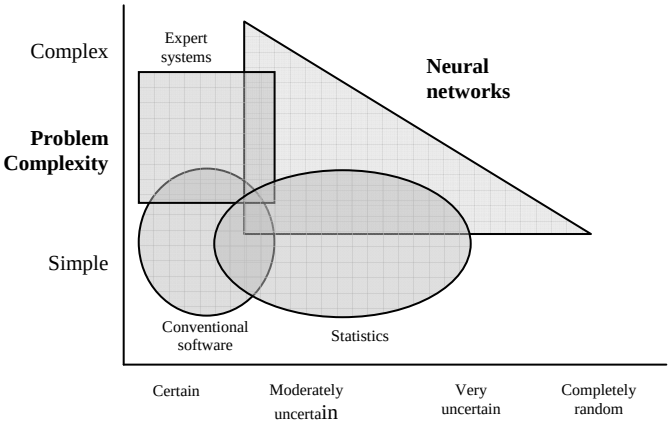

Figure 4 “Applying neural networks to solve problems”

Advantages Neuron networks include:
Adaptive learning - Neural network can learn how to do tasks based on the data given for training or initial experience.
Self-organization - Neural network can create its own representation of the data set it receives during training time.
Real-time operation - Neural network can rapidly go through millions or billions of simulations to train the data set in parallel.
To use neural networks in a real-time risk identification and prediction module, the first step is to formulate the problem. As shown in figure 5, the first step is to select a problem that is suitable for an artificial neural networks. As mentioned, suitable business applications fall into three categories:
Classification problems - Fraud detection, loan approval, loan default and credit card applications fall into this category.
Time series applications - Financial forecasting, stock market prediction, bankruptcy prediction, bad debts estimation, sales and expense forecasting are examples of business applications in this category.
Data mining applications - Many marketing applications fall into this category, such as looking for patterns in customer databases, targeting customers, estimating responses and analyzing demographics.
Basically, an neural networks computer software model is constructed and “trained” from a database of

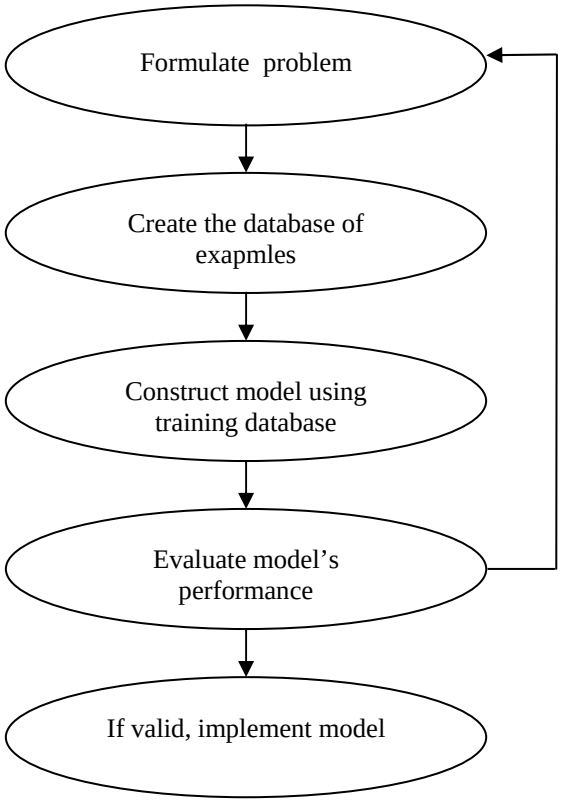

Figure 5 “Detecting risk level using neural networks”

historical examples of input and output variables. During model training, an neural networks learns the patterns and correlations from a sample of input and output data representing actual fraud occurrences and nonfraud occurrences, respectively. The creation of the database is the most important step in the neural networks developmental process. The input and output values are keyed into the neural networks package to construct a network that can then be used by an accountant to make a decision about the possible occurrence of fraud.

8. CONCLUSIONS

The real-time risk management system will be able to teach itself by using neural networks and make decisions which vulnerability can be addressed to which risk value.

For a system where this solution is proposed, there are a few problems that might slow down the implementation of real-time risk management:

- Not all systems are creating log files (some of them are old),
- Not all audit files are the same format (program or tool is needed to make log files understandable for automatic risk assessment system).

This means that at first, the most important systems to organization should be able to create audit files.
The main purpose for this real-time risk management system is to start an effective risk management in

organization and prevent risks before they reached unacceptable value, therefore save money.

References

1. Minkevics V., Slihte „Search for effective risk management" Science proceedings of Riga Technical university; „Computer science", 5.ser., 20.sēj., Rīga, RTU, 2004, p174.-180..(ISSN 1407-7493)
2. Minkevics V., Slihte J.,Vulfs G. „Modelling risk management for unified threat management systems" 19th European Conference on Modelling and Simulation Riga 2005 144.-150.lpp.(ISBN 1-84233-112-4)
3. Minkevics V., Slihte J.,Vulfs G. „Modelling risk management system using neural networks" Science proceedings of Riga Technical university; „Computer science",, 5.sēr., 23.sēj., Rīga, RTU, 2005, p66.-72.(ISSN 1407-7493)
4. Use of real-time risk management in organization" Science proceedings of Riga Technical university; „Computer science",, 5.sēr., 28.sēj., Rīga, RTU, 2006, p23.-29.(ISSN 1407-7493)
5. SANS Institute 2002 "A Guide to Security Metrics"
6. Inductive Solutions, Inc. "An introduction to Risk Management" 2001
7. 2003 C & A Security Risk Analysis Group http://www.security-risk-analysis.com/cobkbs.htm
8. "Inforation Systems Control" Volume 1 2005 "The Role of Attack Simulation in Automating Security Risk Management" by Gidi Cohen "The role of attack simulation in Automating Security risk management" p(51-54).
9. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol1/cs11/article1.html

