ISSN 1407-7493 COMPUTER SCIENCE DATORZINĀTNE 2008-7493

INFORMATION TECHNOLOGY AND MANAGEMENT SCIENCE
INFORMĀCIJAS TEHNOLOĢIJA UN VADĪBAS ZINĀTNE

REAL-TIME RISK MANAGEMENT MODEL

Vladislavs Minkevics, Mg.sc.ing., Ministry of Finance, Smilšu 1, Riga LV 1919, Latvia, e-mail: Vladislavs.Minkevics@fm.gov.lv

Girts Vulfs, Prof., Dr.sc.ing., Riga Technical University, Kaļķu 1, Riga -1658, Latvia, e-mail: vulfs@itl.rtu.lv

Keywords: Real-time risk assessment, associative approach, k-nearest neighbours, real-time risk management system

1. Introduction

Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT – related risk.
One of the most important activities is to perform comprehensive risk analysis and to define effective risk mitigation methods. Effective risk mitigation requires expert who is performing risk analysis to be very competent. Sometimes there is not enough information and time for an expert to evaluate one or another risk.

2. Problem

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization [1]. If business wants actual information about possible threats that may exploit vulnerabilities and risks associated with it, IT risk management must be done on real-time basis.
Based on prior publications, it is known that there is a direct correlation between risk assessment cycle and risk level, because the longer the assessment cycle time, the more exposed the organization is to attacks on critical information assets.

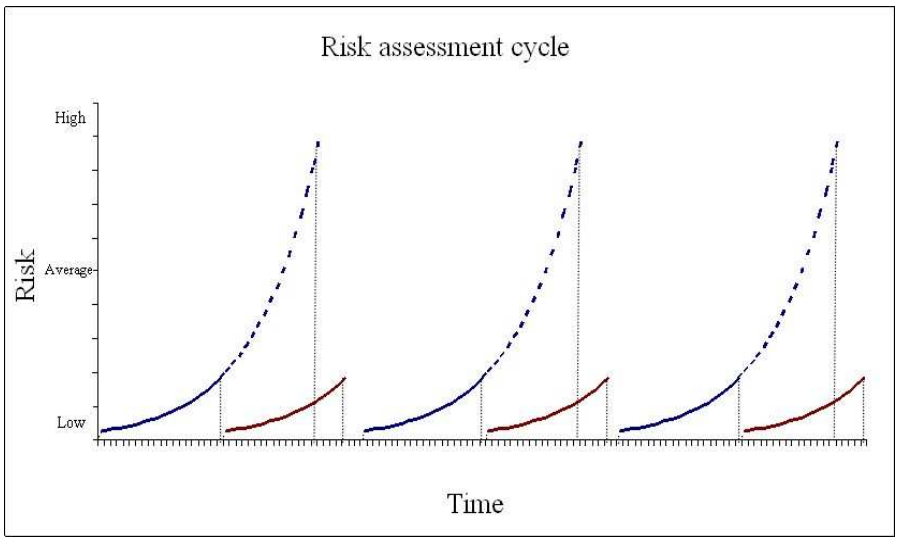

Figure1. Risk assessment cycle

Another aspect to introduce real – time risk management is the level of effort, carried by the security related personnel (Figure 2) where the most is needed to carry out the detailed risk analysis [2].

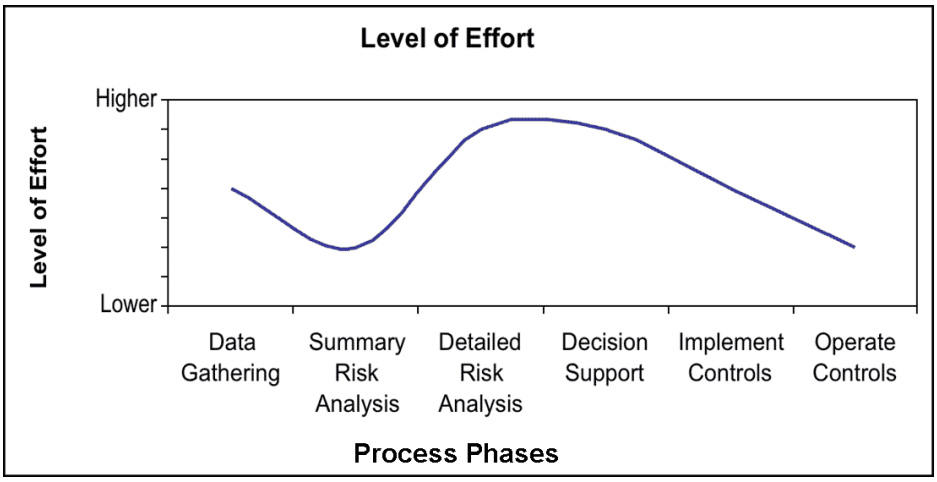

Figure 2. Level of effort during risk assessment phases

3. Real – time risk management

There are several advantages of using real – time risk management. First, being based on artificial intelligence, it is able to teach itself and identify risks based on known experience. Secondly real – time risk management can notice risks instantly, before any threat can exploit the vulnerability. The only disadvantage of using real – time risk management system is that it can analyze risks for systems that can produce audit log files and is not able to analyze risks for such things as:

- back-up practice and policy;
- the contents of the recovery plan;
- the status of the recovery plan;
- general contingency practice, procedures and policies;
- application contingency [3, 4].

These things should be left for experts, therefore the best protection of information assets would be to combine real-time risk assessment with risk management done by experts.

4. Practical solution

In practice the real – time risk management using k-nearest neighbours would need to be applied to log files, generated by systems (Figure 3).

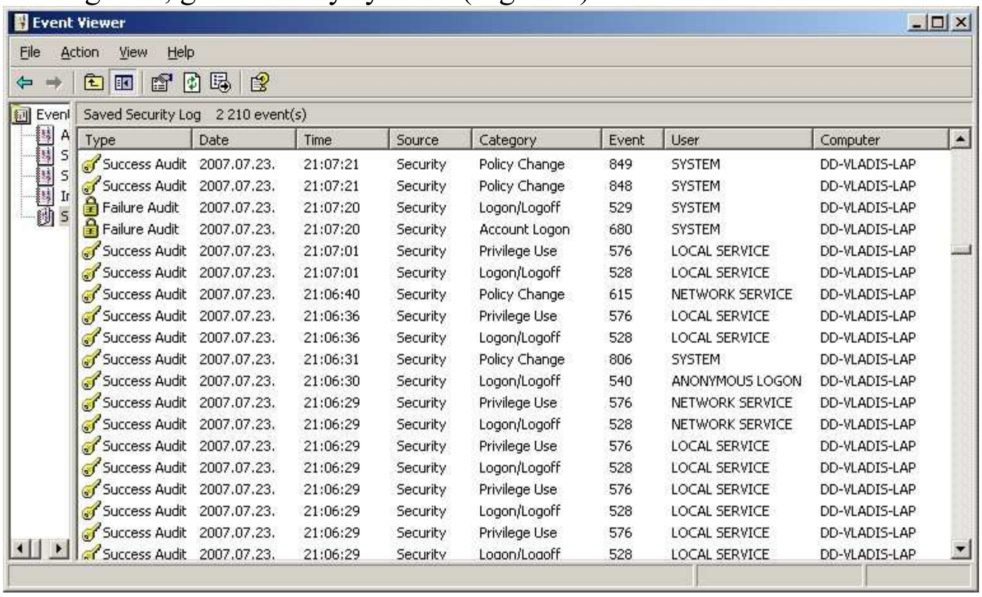

Figure 3. Log file of a system

The next step is to represent audit logs in binary form (Table 1).

Table 1

Binary representation of a system's audit log

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
1	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0
2	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	0
3	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	0
4	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0
5	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	1
6	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
7	1	1	0	0	0	0	0	0	1	0	1	0	0	1	0	0
8	0	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0
9	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0
10	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0

Table 2

X coordinates representation

Internal process	a
Accessing data	b
Authentication in system	c
Use of privilege	d
Change of windows components	e
Password change	f
Username change	g
Change of user class	h
Access to log files	i
Deleting audit log files	j
Repeats at least 3 times in last 15 minutes	k
User is authenticated	l
Access to network	m
Data read	n
Data write	o
Data delete	p

Table 3

Action and Vulnerability associated with it

No.	Coefficient	Action	Vulnerability
1	0,9	User class has been changed	Possible giving unauthorized privileges
2	0,7	Reading audit log files	Possible unauthorized viewing of log files
3	0,8	Unsuccessful attempts to logon	Possible password guessing
4	0,5	The username has been changed	Possible trace misleading
5	0,4	Trying to delete audit log files	Possible trace misleading after attack
6	0,2	Password change	Possible simple password change
7	0,6	Unidentified user tries to read audit files	Possible unidentified log file reading
8	0,1	Accessing network	No vulnerability, just accessing network
9	0,3	User logs into system from home	Vulnerability is small, user tries to logon to system from home behind firewall
10	1	Unauthorized user class change to admin	Possible attack planning

In Table 4 and Table 5 each situation is compared to unknown situation and using Euclidean distance; the closer this situation is to the unknown situation, the smaller distance is reported. Then the distance is multiplied by the coefficient and we have a parameter which describes the closest and most dangerous vulnerabilities which may be addressed to the unknown situation.

Table 4

Searching for k – nearest neighbors in unknown situation (Example 1)

x\y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Distance	Closest	Coefficient
1	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0	6	6,666	0,9
2	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	0	6	8,5714	0,7
3	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	0	10		0,8
4	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	7		0,5
5	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	1	6	15	0,4
6	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	8		0,2
7	1	1	0	0	0	0	0	0	1	0	1	0	0	1	0	0	7		0,6
8	0	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0	6	60	0,1
9	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	8		0,3
10	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	9		1

?	1	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	min=	6,666

From Table 4 it can be seen that four neighbors had the same distance to the new object, where we use the coefficient to find out the most important to us neighbor.

Table 5

Searching for k – nearest neighbors in unknown situation (Example 2)

x\y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Distance	Closest	Coefficient
1	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0	9		0,9
2	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	0	5		0,7
3	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	0	7		0,8
4	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	8		0,5
5	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	1	3	7,5	0,4
6	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	7		0,2
7	1	1	0	0	0	0	0	0	1	0	1	0	0	1	0	0	8		0,6
8	0	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0	3	30	0,1
9	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	7		0,3
10	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	8		1

?	0	1	0	1	0	0	0	0	0	1	0	1	1	1	0	1	min=	7,5

This experiment shows the minimal distance, based on the k-nearest neighbors algorithm. New situation shown in Table 4, according to nearest neighbors, is the closest to situation No.1. In this case, this means that risk of "giving unauthorized privileges" has increased. In unknown situation shown in Table 5, the system has classified it as situation No 5. This means risk of possible audit files deletion has occurred. This experiment shows that the associative approach, and k – nearest neighbors, in particular, may be used for developing real – time risk management system.

5. Model of real-time risk management system

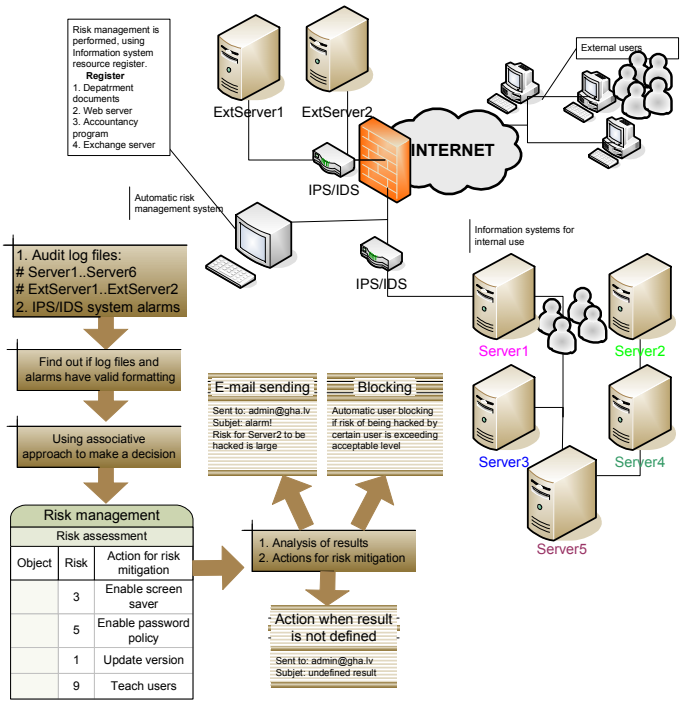

Figure 4. Model of real – time risk management system

Figure 4 shows a model of real-time risk management system location in organization's network. Main part of the system is decision making part. One of the options for it may be the associative approach with k-nearest neighbors as a decision making algorithm. The main advantage of k-nearest neighbors is that it is easy to understand, and experts who are creating all rules for automatic risk management system may define main properties of each vulnerability and the system will automatically sort them into classes from which we can gain risk level of one or another threat (Figure 4) [5-9].

References

1. NIST Special publication 800-30 *Risk management Guide for Information Technology systems* p.1 2002.
2. Microsoft Tech Net „Security Risk Management Guide" 2004 http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/srsgch02.mspx#E1C
3. K.Rigby. *Risk management*. 2003 http://sparc.airtime.co.uk/users/wysywig/risk_1.htm
4. 2003 C & A Security Risk Analysis Group http://www.security-risk-analysis.com/cobkbs.htm
5. Minkevics V., Slihte. Search for effective risk management. *Scientific Proceedings of Riga Technical University. Computer Science. Information Technology and Management Science*, Series 5, Vol. 20, Rīga, RTU, 2004, p.174.-180.(ISSN 1407-7493)
6. Minkevics V., Slihte J.,Vulfs G. Modelling risk management for unified threat management systems. *19th European Conference on Modelling and Simulation*, Riga 2005, p.144.-150.(ISBN 1-84233-112-4)

7. Minkevics V., Slihte J.,Vulfs G. Modelling risk management system using neural networks. *Scientific Proceedings of Riga Technical University. Computer Science. Information Technology and Management Science*, Series 5, Vol. 23, Rīga, RTU, 2005, p.66.-72.(ISSN 1407-7493)
8. Minkevics V., Slihte J.,Vulfs G. Use of real-time risk management in organization. *Scientific Proceedings of Riga Technical University. Computer Science. Information Technology and Management Science*, Series 5, Vol. 28, Rīga, RTU, 2006, p.23.-29.(ISSN 1407-7493)
9. 2003 C & A Security Risk Analysis Group http://www.security-risk-analysis.com/cobkbs.htm

Minkevičs Vladislavs, Vulfs Ģirts. Reāla laika riska menedžmenta modelis
Šis raksts ir par iespējamu veidu, kā uzlabot vienu no svarīgākajām jomām informācijas tehnoloģijās – risku analīzi. Risku analīzei jābūt kā proaktīvam rīkam, lai minimizētu zaudējumus, kas varētu rasties no drauda, kurš izmantojis apdraudējumu. Kopējais risks var tikt minimizēts gadījumos, ja tiek pamanīti apdraudējumi agrā stadijā, kas nozīmē, efektīvai risku analīzei nepieciešams risku analīzi veikt regulāri. Ir grūti apskatīt visus iespējamos apdraudējumus risku analīzes gaitā. Ekspertiem analizējot riskus ir jāveic process, kas atkārtojas un ir ļoti nogurdinošs. Mākslīgais intelekts ir viens no rīkiem, kuru var izmantot, lai analizētu riskus reālā laikā un noņemt no ekspertu pleciem tos apdraudējumus, kas bieži atkārtojas. Protams mākslīgais intelekts nav izmantojams analizējot tādus riskus, kā procedūru pilnība un to atbilstība normatīvajiem aktiem. Rakstā tiek piedāvāts dalīt risku analīzi divās daļās – vienu izmantojot ekspertus, otru – mākslīgo intelektu. Rakstā parādīts piemērs, kā izmantojot k- tuvāko kaimiņu metodi ir iespējams noteikt nezināma apdraudējuma iespējamo draudu.

Minkevics Vladislavs, Vulfs Girts. Real-time risk management model
The paper is about a way to improve one of the most important areas of information technology – risk assessment. Risk assessment must be as a proactive tool which minimizes loss in case when threat exploits vulnerability. The overall risk can be minimized when vulnerabilities are noticed in early stages, which means that for effective risk management, it must be done on regular basis. As a matter of fact, it is very hard to cover all vulnerabilities in risk assessment. Experts should go through the repeated and boring process when analyzing possible vulnerabilities and threats and risk associated with them. Artificial intelligence is one of the tools which can be used to analyze risks on real-time basis and take off the most repeated vulnerabilities. Of course, artificial intelligence can't be used to analyze such risks as security procedures and regulation compliance. The paper describes a way to divide risk management into two parts – one should be done by experts and the other one – by the artificial intelligence. Artificial intelligence is used to classify vulnerabilities and create a real – time risk analysis based on prior knowledge. The paper shows an example how the classification and analysis could be done using the associative approach with k-nearest neighbours.

Минкевич Владислав, Вульф Гирт. Модель системы менеджмента рисков в реальном времени
В данной публикации речь идет о возможности улучшения одной из самых важных сфер информационных технологий – анализа рисков. Анализ рисков должен быть проактивным инструментом, который помогает избежать больших финансовых потерь в результате возникновения риска. Общий риск может быть минимизирован только в том случае, когда анализ рисков производится постоянно. Ведение непрерывного анализа рисков представляется возможным только с помощью средств информационных технологий. Одним из возможных решений при обеспечении непрерывного анализа рисков является использование ассоциативных методов, а именно метод к-ближайших соседей. Безусловно, применение искусственного интеллекта, с помощью которого можно анализировать наиболее повторяющиеся риски, не представляется возможным при оценивании процедур, а также их соответствия нормативно-правовым актам. Поэтому, эффективный анализ рисков включает в себя как автоматизированную, так и дополнительную мануальную оценку рисков. В статье приведен пример использования метода принятия решений, основанного на методе к-ближайших соседей для анализа рисков в реальном времени.