ICT SECURITY MANAGEMENT

Jeanne Schreurs, Rachel Moreau
Universiteit Hasselt
Agoralaan
3590 Diepenbeek.
Belgium.

jeanne.schreurs@uhasselt.be
rachel.moreau@uhasselt.be

KEYWORDS

Security, Risk

ABSTRACT

Security becomes more and more important and companies are aware that it has become a management problem. It's critical to know what are the critical resources and processes of the company and their weaknesses. A security audit can be a handy solution. We have developed BEVA, a method to critically analyse the company and to uncover the weak spots in the security system. BEVA results also in a general security score and security scores for each security factor. These will be used in the risk analysis.
The goal is to increase the security score Ss to a postulated level by focusing on the critical security factors, those with a low security score.
We will identify the critical threats too, being those with a high risk or expected loss for the company if they occur.
In the next stage it will be resolved to implement some security measures to decrease the probabilities of the occurrence of the threats and as a consequence to decrease the risks and to improve the security situation.

1. ICT SECURITY MANAGEMENT

As a consequence of the fast integration of technologies as Internet, Intranet, Extranet, Voice over IP and e-commerce, a companies ICT-infrastructure will move to more openness to the outside world and as a consequence will become more vulnerable for security threats. This offers lots of new opportunities but also creates new threats. That's why focus and responsibility concerning security become even more and more important. Studies show that attacks come from inside as well as from outside the organisation and bring along large costs. Because of these large costs, companies became more and more aware that they not only deal with a technical problem but also with a management problem.

ICT-security management consists of a security audit activity and of a risk analysis. Both topics will be discussed in this paper.

2. SECURITY AUDIT

Spending each year a certain amount on security measures is not enough. A company needs a total security approach. It is a must to know what are the critical resources and processes of the company and their weaknesses. A solution to this is a security audit. Based on the results of the audit, a security policy can be developed , adjusted to the company situation. A security audit can be used to analyse and describe the security level.

2.1. Our security audit checklist

We have developed a security audit, called BEVA. BEVA is a method to analyse critically the company and to uncover the weak spots of the security system.
We have developed a standard list that covers all aspects of security in the different areas or of business functions. Each of these areas consists of different security factors. The factors are in their turn tested on the basis of several questions.

We based our security analysis partly on the Marion-AP method. But our list for the security factors is based on the standard ISO 17799. The 36 security factors are spread over the 10 domains , as set forward in the standard ISO17799 model. For example you have the domain "system access control" and in this domain you have the factors: requirements for access, management of user access, user responsibility, control of network access, control access to OS, control of access to applications and information and use of mobile infrastructure.
For each of the 36 factors, a number of subcriteria are formulated. We developed a list of questions, covering the subcriteria we created. The questions are partly based on the "checklists in information management" SDU publishers. (www.riskworld.net/7799-2.htm)

Security Factor Sfi	Importance	Sub Factor	Relevance/weight 1 to 4	Code question	Question	evaluation 1 to 4
Domain: Access control						
Sf20. Business requirements for access controlPremise	B	access control policymanagement	3	20.1	Is the access control policymanagement based on the business security requirements?	3
				20.2	Are aspects of logical and physical access control included?	3
				20.3	Is it clear for users and service providers which rules are applicable?	2
Sf21. User access management	C	registration of users	2	21.1	Is there any formal user registration and de-registration procedure for granting access to multi-user IS and services?	1
		privilege management	1	21.2	are privileges and allocated on need-to-use basis?	3
				21.3	are privileges only allocated after formal authorisation process?	1
		user password management	4	21.4	should the allocation and the reallocation of passwords be controlled through a formal management process?	3
				21.5	are the users asked to sign a statement to keep the password confidential?	1
		review of user access rights	3	21.6	does there exist a process to review user access rights at regular intervals?	4
					Does there exist a procedure to block the	

Figure 1: Questions audit checklist

Security factor Sfi	Security Subfactor Ssfij	Relevance /weight 1 to 4 w(i,j)	Code question	evaluation 1 to 4	mean evaluation 1 to 4 eval(i,j)	Security factor score Sfis
Domain: Access control						
Sf20. Business requirements for access controlPremise	access control policymanagement	3	20.1	3	2,67	2,67
			20.2	3		
			20.3	2		
		3				
Sf21. User access management	registration of users	2	21.1	1	1	2,25
	privilege management	1	21.2	3	2	
			21.3	1		
	user password management	4	21.4	3	2	
			21.5	1		
	review of user access rights	3	21.6	4	3,5	
			21.7	3		
		10				
Sfis = sum [(w(i,j) * eval(i,j)] / sum w(i,j)						

Figure 2: Calculation of the Sf I's

2.2. The audit process and the calculation of security factor scores Sfi's and the security score Ss

To collect the information about the current security situation of the company, we start with the questioning of the key persons in the company using the audit checklist questionnaire.
The company determines which systems or processes are critical for them and connected with it, which security factors are important or relevant.

An importance rate is given to the security factors from A (low importance) to E (high importance). Next a weight between 0 and 4 is allocated to the subcriteria of the security factors to indicate the relevance.
Subsequently the evaluation starts and each question is given a score between 1 and 4 (see figure 1).

Sfi s = sum [eval (i,j) * w(i,j)] / sum w(i,k)

Ss= sum [eval (1,36) * w(1,36)] / sum w(1, 36)

For example see factor 21 in the example:
[2*1 + 1*2 + 4*2 + 3*3,5]/10 = 2.25
Ss= in this example 2.66

Security Factor	Weight	Sfi	Security Factor	Weight	Sfi
1	A	2,25	19	B	3,5
2	D	3,33	20	B	2,67
3	B	2,75	21	A	2,25
4	A	3	22	D	2
5	C	1,75	23	E	2,33
6	D	2,33	24	C	2
7	A	2,25	25	A	2,67
8	B	3,25	26	D	2,5
9	E	2,33	27	B	1,75
10	D	2,67	28	E	3
11	C	2	29	B	3,25
12	A	3,67	30	C	3,33
13	C	3	31	B	2,75
14	B	2,5	32	C	2,67
15	D	1,67	33	A	2
16	A	2,67	34	E	2
17	E	3,33	35	C	2,5
18	C	2,25	36	B	3

Figure 3: Sfi's results

Based on the evaluated questionnaire and the allocated weights, a realistic picture of the security situation of the company can be created as well general as by factor. This is showed graphically in BEWA, see figures below. Figure 5 highlights which security factors are crucial, and points out the security factors which need immediate attention by placing them in the red area.

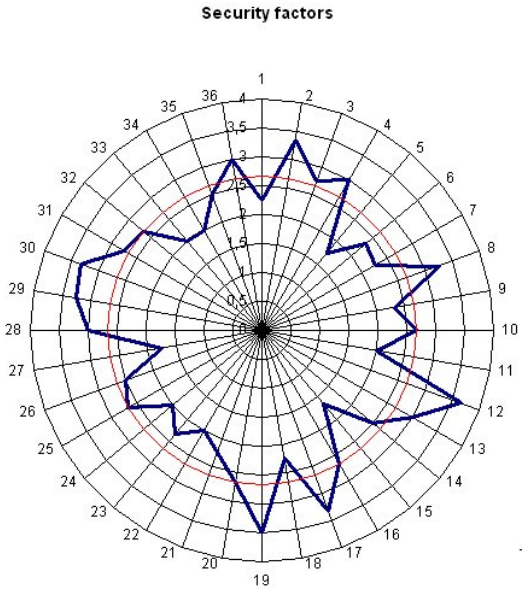

Figure 4: Graph of the security scores

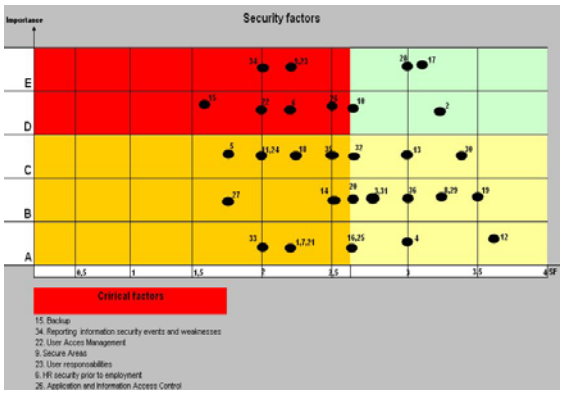

Figure 5: Graph of security factors and their importance

Feedback is given to the company and the evaluation states immediate points of action.
A list of action points is created. Taking into account the stated security budget and the factors and their importance, an action plan is suggested.

3. RISK ANALYSIS

As stated earlier ICT security management is based on a security audit and on a risk analysis. The security audit gives us an average security score Ss for the enterprise and a SFi for each of the security factors as explained in the previous chapter. In this part we will take a closer look at the risk analysis and use the outcomes of the security audit to do our risk analysis. Our risk analysis is partly based on the Marion-AP method.

3.1. Potential losses linked with the occurrence of threats.

Companies loose large amounts of money on violations. A table which states the relation between the threats and the types of incurred losses is constructed.

Losses due to the occurrence of threats or security risks have to be measured in the company.

Threats	Function in the company				Loss
	Type of loss 1	Type of loss 2	Type of loss 3	…	
T1= Virus	x		x		L1
T2= Laptop/ mobile theft	x				L2
T3= Insider abuse of net access		x			L3
…					

Figure 6: Threats versus losses

As types of loss we choose the categories :

- material damages and supplements
- additional costs and exploitation losses
- loss of money and material
- other losses

Other categories are possible. But what we are interested in, is the total loss for each risk (being L1, L2,L3,…).

3.2. Probability of risks

The yearly organised CSI/FBI-study delivers the following probabilities for the threats:

Threat	(CSI/FBI 2006)	Kans	(CSI/FBI 2006)
T1	Virus	Pt1	0.65
T2	Laptop/mobile theft	Pt2	0.47
T3	Insider abuse of net access	Pt3	0.42
T4	Unauthorised access to information	Pt4	0.32
…		…	

Figure 7: Probability of risks

3.3 The risks of the threats and the list of critical threats

Our final goal is to influence the occurrence of the threats, or the probability of the occurrence of them, by implementing selective security measures in the company. This will impact in the long run the security situation.
We must concentrate on the critical security factors, following the results of the audit. If the security factor is critical, than the threats linked with it have a critical risk too.

In figure 7 we figure out the relations between the threats and the security factors.

Th	Security factors					
	Sf1 …	Sf20: require-ments for access	Sf21: mgt of user access	…	Sf36
T1	x	x			
…					x
T4		x	x		
T5	x				
…					

Figure 8: Relations between security factors and threats

We can base our study on the probabilities found in the CSI/FBI study
We assume that the probabilities in the CSI/FBI study are averages of the security situation of a large number of companies.
Our company's security score Ss can be seen as a representative of this average situation and so the probabilities can be interpreted as being prior probabilities of our company's security situation.
We can recalculate the probabilities of the threats by weighing them with the corresponding security factor scores Sfis of the related security factors.

The security score of the threat j = STjs

Taking into account the individual security factor scores Sfis of those security factors which have a positive relation with the threat, we need to adjust the probability .
By calculating the average security score of each threat and their adjusted probability.

Threat	Ssi / Probab.	Security factors				Ss	Average Secur. score Risk	Adjusted proba-bility
		Sf1	Sf2	Sf3	…			
		Ss1	Ss2	ss3				
T1	P1	x		x			SsT1	P1'
T2	P2				x		SsT2	P2'
T3	P3	x	x	x			SsT3	P3'
…								

Figure 9: Adjusted probability of the threats

SsT1= the sum of all the scores of the questions of the factors that have a relation with T1 divided by the the assigned weight of those factors;
Pi = (1-Pi)* SsTi/Ss

After calculating the adjusted probability, we can now calculate the risks of the threats for our company.

Threat	Probability	Loss	Risk
T1	P1'	L1	P1' * L1
T2	P2'	L2	P2' * L2
T3	P3'	L3	P3' * L3
T4	P4'	L4	P4' * L4
…			

Figure 10: The risk of the threats

In this table we can identify the critical risks, or the threats raising a high risk for the company.

4. DECISION ON SECURITY MEASURES

The next stage is to resolve on to security measures. First a table wit the most used measures along the CSI-study.

Most used measures (CSI-study)
Firewall
AntiVirus Software
AtiSpyware Software
Server Based Acces control list
Intrusion detection system
Ecryption for data
Reusable account system
Intrusion prevention system
Log management software
Application level firewall
Smart card/one time password token
Specialized wireless security
Training personel
Endpoint security client software
Update server
Firewall
AntiVirus Software
AtiSpyware Software
Server Based Acces control list
Intrusion detection system

Figure 11: Most used measures

The critical threats should be restrained by taking the necessary safety requirements. For each of the threats a security measure can be taken but it is also possible that one measure can resolve or effect several threats. It's important to evaluate the costs of the measures and the possible loss of a threat. It is obvious that the cost can't be higher than the expected loss.

	Threats Ti				
Measures	T1	T2	T3	…	Costs
M1= firewall				X	C1
…		x	x		C2
					…
M14	x				C14
M15	x				C15

Figure 12: Measures for the different threats

5. FOLLOW UP

After a period of approximately 3 months after implementing the security measures, a new security audit should be taken. The new security score Ss is calculated and compared to the stated aimed Security score using the security measures.
If there are security factors that score too low, these should be investigated and adjusted;

REFERENCES

- Jean-Marc Lamère: la sécurité informatique; Dunod : La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux)
- www.eisti.fr/~bg/COURSITACT/TXT/m_marion.txt
- Information Security Management ; BS ISO/ IEC 17799:2005 ; SANS Audit Check List: author: Val Thiagarajan B.E., M.Comp, CCSE, MCSE, SFS, ITS 2319, IT Security Specialist.
- (www.riskworld.net/7799-2.htm)
- 2006 CSI/FBI-study about cybercrime: COMPUTER CRIME AND SECURITY SURVEY: by Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson
- https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=27372&sessionid=1&key=42F39B89EE0B30BA951711A5E7A98EDD&sourcepage=register
- http://mediaproducts.gartner.com/gc/webletter/computerassociates/vol3issue3_risk/index.html
- Security Management: A New Model to Align Security With Business Needs; Sumner Blount, CA Security Solutions ;August 2006