ICT SECURITY MANAGEMENT AND RISK MANAGEMENT

ICT SECURITY MANAGEMENT AND RISK MANAGEMENT

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

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

KEYWORDS

Security, Risk

ABSTRACT

It's critical to know what are the critical resources and processes of the company and their weaknesses. Security has become a management problem. A security audit can offer a handy solution. We have developed a method and a system. The system is called BEVA. BEVA includes a security audit measuring the security situation of the organisation in 38 security factors. Based onthis audit, it delivers an overall security score and the one for each security factor. It also supports management in detecting the critical security factors in the company. The ICT security budget is not unlimited. As a result not all needed security technologies can be implemented to improve all critical SF's. To create a priority list of the corresponding critical threats we need to refer to organisational risks. We calculate the company specific risk scores and by the way we identify the most critical threats and by the way the most effective security technologies that must be implemented

1. SECURITY AUDIT

1.1. ICT security is a management issue

As a consequence of more openness to the outside world, companies become more vulnerable for security threats. Studies show that some attacks bring along large costs. That is why companies become more and more aware that ICT security is a management problem. (9),(12) Actually a company needs a totally 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.

1.2. Security audit

We have developed a security audit, called BEVA. It is covering the 10 domains as set forward in the ISO17799 model. (3) BEVA is a method to analyse critically the company and to uncover the weak spots of the security system. It positions the company on point of the security aspects in the different areas of business functions. We have developed a standard list that covers all aspects of security, structured in 10 domains.

Each of these areas consists of different security factors. In total 38 security factors are spread over the 10 domains. For each of the 38 factors, a number of subcriteria are formulated. (4), (13), (14) We developed a list of questions, covering the subcriteria we created. The questions are partly based on the "checklists in information management" SDU publishers.

10 domains
- Security policy - Organization of information security - Asset management - Human resources security - Physical and environmental security - Communications and operations management - Access control - Information systems acquisition, development and maintenance - Information security incident management - Business continuity management

2. THE AUDIT PROCESS AND SECURITY DECISION MAKING

2.1. Our security audit checklist

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 38 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: Sf20 requirements for access, Sf21 management of user access, Sf22 user responsibility, Sf23 control of network access, Sf24 control access to OS, Sf25 control of access to applications and information and Sf26 use of mobile infrastructure. (Figure 1)

We start with the questioning of the key persons in the company using the audit checklist questionnaire.
An importance rate is given to the security factors from A (low importance) to E (high importance) (figure 1).
For each subfactor a relevance score from 1 to 4 has to be given and each question has to be evaluated by a score between 1 and 4. For each subfactor a relevance score from 1 to 4 has to be given and each question has to be evaluated by a score between 1 and 4. When the questionnaire is completed, BEVA now calculates the security factor scores Sfis. If all the factor security scores are calculated also an overall security score Ss is given;

2.2. The calculation of security factor scores Sfis and the overall security score Ss (Figure 2).

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	Sub Security Factor	Relevance/weight 1 to 4 w (i,j)	Code	Evaluation 1 to 4	Mean evaluation per Sf 1 to 4 eval (i,j)	Security factor security score Sfis
Security domain : Access control						
1. Requirements for access control	Access control policy	3	2.1.1	2		
			2.1.2	3		
			2.1.3	2	2,33	2,33
		3				**2,33**
2. Management of User access	User registration	2	2.2.1	3	3,00	
	Privilege- management	1	2.2.2	2		
			2.2.3	1		
			2.2.4	2		
			2.2.5	3	2,00	
	User password management	4	2.2.6	4		
			2.2.7	1		
			2.2.8	2		
			2.2.9	3		
			2.2.10	4		
			2.2.11	3	2,83	
	Review of user access rights	3	2.2.12	2		
			2.2.13	2	2,00	2,46
		10				**2,46**
Security factor score: $Sf_{is} = \Sigma [(w(i,j) * eval(i,j) / \Sigma w(i,j)]$						
Security score: $Ss = \Sigma_i \Sigma_j [w(i,j) * eval(i,j)] / \Sigma i \Sigma j\, w(i,j)$						

Fig. 2. Calculation of security scores

In BEVA, we express the state of security into scores of the security factor (Sfi's). We do this for all the factors and in the end we give a general security score (Ss) over all security factors. We based our security analysis partly on the Marion-AP method.

The management team evaluates the company for all aspects on a one to four scale and at the same time measures the importance or relevance of all subfactors.
For all security factors Sfi, I=1,38 one or more subfactors do exist: SSfij, j=1,k.
For each subfactor one or more questions are included in the audit questionnaire.
Eval(i,j) is the evaluation of the subfactor Ssfij and is the mean value of the evaluations for the individual questions, corresponding to that subfactor.
W(I,j) are the weights and corresponds to the measure of relevance for the subfactors.
The security factor security score Sfis for factor Sfi is the evaluation of the security of the security factor Sfi and is equal to the weighted mean of the evaluations of the subfactors:
Sfi s = Σj [eval (i,j) * w(i,j)] / Σ w(i,j)
The overall security score Ss requires the weighing over all Sf evaluations and using the total weight:
Ss= Σi Σj [w (i,j) *eval (i,j)] / ΣiΣj w(i,j)

For example for the security factor management of user access see figure 2; it has a security factor score of 2.46;
The security score Ss is in this example = 2.39
Figures 3 and 4 show the scores of all the security factors. The red line in figure 5 states Ss the overall security score. The blue line connects the individual scores of the security factors. In the graph of Figure 4 the factors with score weaker than the company mean or overall security score can be identified
Based on these reports management can decide to concentrate on those security factors. Indeed if the situation on those points can be improved, as a consequence the overall score will increase too, and so the overall security of the company.

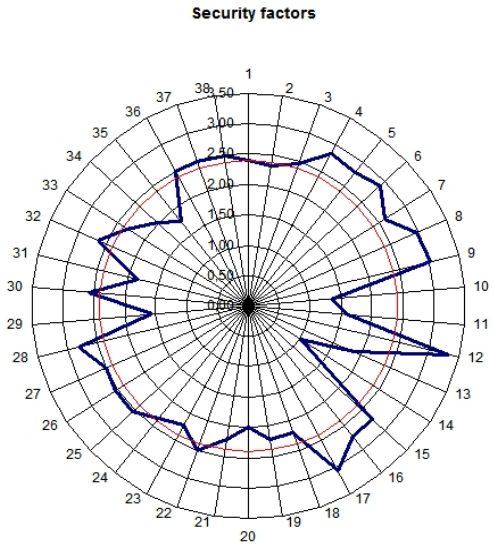

Fig. 3. Graph of the security scores

Security factor	weight	SfiS	Security factor	weight	Sfi
1	A	2,38	20	B	1,98
2	D	2,33	21	B	2,21
3	B	2,46	22	A	2,50
4	A	2,83	23	D	2,21
5	C	2,76	24	E	2,33
6	D	2,90	25	C	2,56
7	A	2,60	26	A	2,56
8	B	2,96	27	D	2,50
9	E	3,00	28	B	2,80
10	D	1,33	29	E	1,55
11	C	1,60	30	B	2,57
12	A	3,30	31	C	1,83
13	C	1,86	32	B	2,62
14	B	1,00	33	C	2,31
15	D	2,72	34	A	2,00
16	A	2,72	35	E	1,75
17	E	3,06	36	C	2,50
18	C	2,20	37	B	2,50
19	B	2,20	38	C	2,50

Fig. 4. Table of security scores for the security factors

2.3. Critical security factors and security decision making

Management has not only evaluated the security but it has also decided about the importance to them of the security factors or the security domains included in the audit.
As a consequence we can use those measures to differentiate between the weak factors as resulting from the previous analysis. We are also creating a report that combines the scores of the security factor with its importance. The differences are well stressed in this graphic and immediate points of action can be stated. (Figure 5)
We identify 4 regions and the Sfi can be found in one of them:

Red	Critical, improvement is urgent
Green	Continuation
Orange	No action/ no concern
Yellow	Not important, but follow up

Figure 5 highlights which security factors are critical, and for which improvement is needed. Critical means being evaluated low and being important. This feedback is given to the company management. Based on it action points can be developed. The goal is to increase the overall security score Ss by improving some low valued individual Sf security score. First we calculate a loss score for all threats. After adjusting the prior probability of occurrence of the threats, we calculate a risk score.

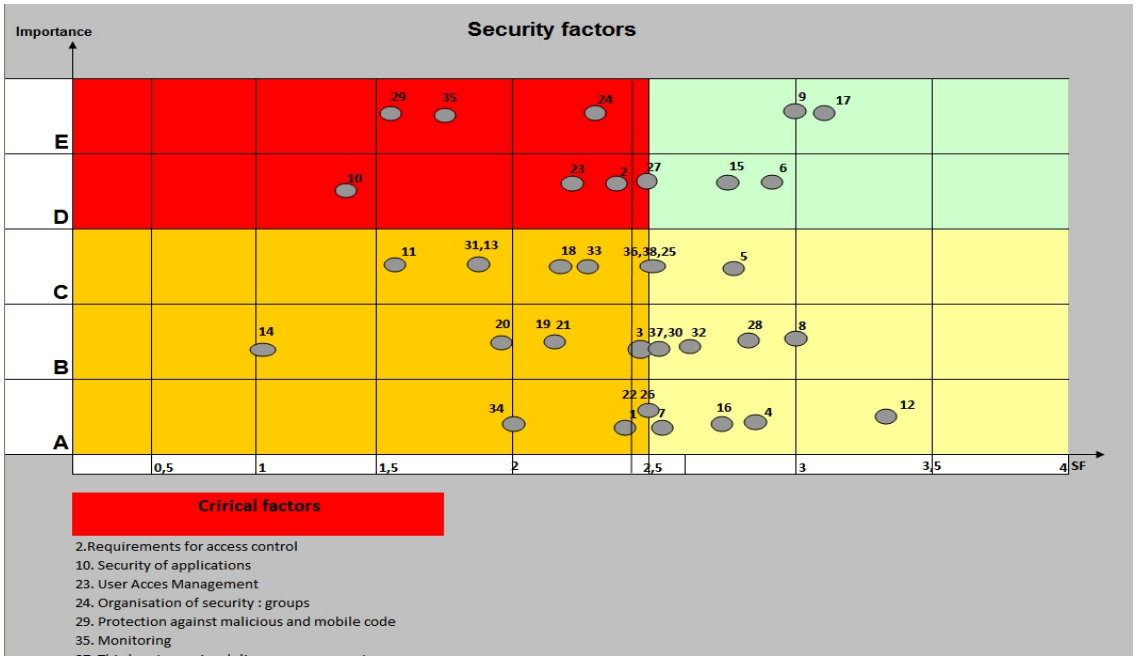

Fig. 5. Graph of security factors and their importance

3. ICT SECURITY DECISION MAKING AND ORGANISATIONAL RISKS

The ICT security budget is not unlimited. As a result not all needed security technologies can be implemented to improve all critical SF's.
We developed an ICT security management system. We developed a new methodology for security management decision making. To improve the security situation we will implement security technologies to decrease the probability of occurrence of the critical threats. (10), (11) first we must identify the critical threats corresponding to the critical security factors. And because not everything can be solved immediately due to a limited budget, we need some procedure to create a list of threats in descending order of probability of occurrence.

3.1. Losses due to the occurrence of threats: loss scores

Based on the table of total losses and on the occurrence percentage (used as the probabilities) of threats (cfr. CSI Survey-Annual Computer crime and security survey), we can calculate a loss score by dividing the total loss by the occurrence percentage. We prefer to work with a loss score instead of the loss itself because first it is very difficult in practice to determine the losses resulting from the occurrence of threats and second we do not need the exact value of the loss, but rather a priority list. The yearly organised CSI/FBI-study delivers the following figures for the occurrence of the threats. Corresponding the exact losses we have calculated a loss score. Index value 100 is given to the highest loss due to "financial fraud";

3.2. Risks due to the occurrence of threats: risk scores

The occurrence level of the threats in the study can be interpreted as being the probability of the occurrence of the threats or the " mean" situation of a company.

Threat	Occurence	Loss score
Financial fraud	0,12	100
Virus	0,52	9,17
System penetration	0,13	30,04
Theft of confidential data, from all causes but mobile device theft	0,25	23,25
Laptop/Mobile theft	0,5	4,41
Insider abuse of net access	0,59	2,78
Denial of Service	0,25	6,56
Phishing	0,26	6,01
Illigal software applications on the system (bots, trojan horses,…)	0,21	7,76
Unauthorised access to information	0,25	2,37
Instant messaging abuse	0,25	0,46

Fig. 6. Loss score for the threats

Threats	Security factors				
	Sf1 …	Sf20: requi-rements for access	Sf21: mgt of user access	…	Sf38
T1	x	x			
…					x
T4		x	x		
T5	x				
…					

Fig. 7. Relations between Sf's and threats

In the analysis of the security situation of our company, we can interpret those probabilities as the prior probabilities. If the overall security score of the company is high, the probability of occurrence of threats will be relative low, as will be figured out in the adjusted and smaller values for the company specific probabilities that will be calculated. We created a table that shows the relation between the treats and the security factors.
To calculate the adjusted probabilities we have to relate the threats with the relevant security factors. Adjustments will be made using the ratio of the mean value of the related Sf's to the Ss.

$$SsTi = \sum_{k=1}^{n} S f_k s / n \times Ss$$

n = number of related security factors to threat i

Pi= prior probability of threat i
1-Pi= prior probability of not-occurrence of threat i
Ss= overall security score
Pi'= adjusted prior probability
Adjustment factor: SsTi
1 - Pi'= SsTi (1- Pi)

We already calculated the loss scores. And because the risk is the expected value of the loss or can be calculated as the loss multiplied by the probability, we can calculate the risk scores of the company by multiplying the loss scores by the adjusted company specific probabilities.
Now we can range the threats in descending order of risk score. Priority will be given to the first categories. Dependent on the budget the most effective security technologies will be implemented, needed to improve the security situation by preventing the company against the occurrence of the threats.

Threat	Pi	1-Pi	SsTi	1-Pi'	Pi'
Financial fraud	0,12	0,88	1,01	0,89	0,11
Virus	0,52	0,48	0,65	0,31	0,69
System penetration	0,13	0,87	0,93	0,81	0,19
Theft of data	0,25	0,75	1,02	0,76	0,24
Laptop/Mobile theft	0,5	0,5	1,07	0,54	0,46
Insider abuse of net access	0,59	0,41	0,90	0,37	0,63
Denial of Service	0,25	0,75	0,87	0,65	0,35
Phishing	0,26	0,74	0,85	0,63	0,37
Illigal software applications on the system (bots, trojan horses,…)	0,21	0,79	0,83	0,66	0,34
Unauthorised access to information	0,25	0,75	0,93	0,70	0,30
Instant messaging abuse	0,25	0,75	0,85	0,64	0,36

Figure 8. Adjusted probability of the threats

Threat	loss score	Pi'	Risk score
Financial fraud	1,00	0,11	10,76165
Virus	9,17	0,69	6,309383
System penetration	30,04	0,19	5,768547
Theft of data	23,25	0,24	5,532846
Laptop/Mobile theft	4,41	0,46	2,043806
Insider abuse of net access	2,78	0,63	1,752233
Denial of Service	6,56	0,35	2,296816
Phishing	6,01	0,37	2,2183
Illigal software applications on the system (bots, …)	7,76	0,34	2,649647
Unauthorised access to information	2,37	0,30	0,70927
Instant messaging abuse	0,46	0,36	0,16436

Fig. 9. Risk score

4. DECISION MAKING ABOUT THE IMPLEMENTATION OF SECURITY TECHNOLOGIES

The next stage is to resolve on to security technologies. First a table wit the most used technologies along the CSI-study.(5) (9)

Most used technolkogies (CSI-study)
AntiVirus Software
Firewall
VPN
AtiSpyware Software
Intrusion detection system
Ecryption for data
Vulnerability/patchmanagement
Server Based Acces control list
Static account login/password
Encryption for data in storage
Smart card/one time password token
Public key infrastructure
Specialized wireless security

Fig. 10 Most used technologies

	Threats Ti			
Security technologies	T1	T2	T3	…
M1= antivirus				X
M2= firewall		x	x	
…				
M14	x			
M15	x			

Fig. 11 Technologies to protect against the threats

The critical threats should be restrained by taking the necessary safety requirements. For each of the threats a security technology can be taken but it is also possible that one technology can resolve or effect several threats. It's important to evaluate the costs of the technology and the possible loss of a threat. It is obvious that the cost can't be higher than the expected loss.
After a period of approximately 3 months after implementing the security technologies, 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 technologies.
If there are security factors that score too low, these should be investigated and adjusted.

5. CONCLUSION

Following the standard ISO17799 model, an audit checklist has been developed. We developed a new methodology for the security management decision making. In the decision model we are using the output figures of the CSI study. A company can now very easily identify its critical security factors and the most serious security threats.

REFERENCES

1. Jean-Marc Lamère: la sécurité informatique; Dunod : La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux)
2. www.eisti.fr/~bg/COURSITACT/TXT/m_marion.txt
3. 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.
4. (www.riskworld.net/7799-2.htm)
5. CSI2007 study about cybercrime: COMPUTER CRIME AND SECURITY SURVEY: by Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson
6. https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=27372&sessionid=1&key=42F39B89EE0B30BA951711A5E7A98EDD&sourcepage=register
7. http://mediaproducts.gartner.com/gc/webletter/computerassociates/vol3issue3_risk/index.html
8. Security Management: A New Model to Align Security With Business Needs; Sumner Blount, CA Security Solutions ;August 2006
9. K.C.Laudon & J.P.Laudon: Management Information Systems. Prentice Hall 2006.
10. Cavusoglu, Huseyin, B.Mishra, S.Raphunathan: "A model for evaluating IT security Investments". Communications of the ACM 47 no7- 2004.
11. D.W.Straub, R.J.Welke: "Coping with systems risk: security planning model for management decision making". MIS quarterly 22 no 4-1998.
12. L.Volonino & S.R.Robinson: "Principles and Practices of Information Security". Prentice Hall 2004.
13. http://www.knowledgeleader.com: internal audit tools and resources.
14. http://www.itcinstitute.com : IT audit checklist information security