"Need-to-know" principle and fuzzy security clearances modelling

Lech J. Janczewski
Department of Management Science and Information Systems, The University of Auckland, Auckland, New Zealand
Victor Portougal
Department of Management Science and Information Systems, The University of Auckland, Auckland, New Zealand

Keywords
Data security, Fuzzy sets, Security, Information, Data protection

Abstract
The paper discusses the assignment of security clearances to employees in a security conscious organisation. New approaches are suggested for solving two major problems. First, full implementation of the "need-to-know" principle is provided by the introduction of data access statements (DAS) as part of an employee's job description. Second, for the problem of setting up border points between different security clearances, the paper introduces a fuzzy set model. This model helps to solve this problem, effectively connecting it with the cost of security.

Information Management & Computer Security
8/5 [2000] 210–217

[ISSN 0968-5227]

Introduction

Managing information security depends on business environment, people, information technology, management styles, time – to list the most important. Within this domain the following seem to be recognised as routine procedures:

- *Development of a strategic plan to protect information resources of the business organisation*. Despite the existence of enough evidence indicating a constantly increasing number of security violations and resulting losses, the majority of business organisations failed to develop their security managing strategic plans. A total of 50 per cent of them do not have even a disaster recovery plan (Jordan, 1999). Without such a plan any effort to tighten up security of information within organisations is a non-optimised procedure.
- *Development of information security policy (ISP)*. ISP is a document that outlines the main checkpoints that are directed specifically at an individual organisation's operations (Forcht, 1994). ISP could be a page or even 200 pages depending on the level of details of the checkpoint procedures (Leung, 1998).
- *Classification of security levels, security clearances and security labels*. This is the domain of the security models, starting from classic Bell-La Padula, Biba and USA Department of Defence Orange Book models. Security levels deal with the classification of information in terms of its accessibility. Security clearances determine the rights of persons/program to access the data. Security labels are a mechanism to match security levels and security clearances.
- *Development of reference monitor*. Virtually every security policy can be modelled in terms of subjects (people and programs) accessing objects (information either in electronic form or hard documents). This view of security policy implies that some decision procedure should exist to decide which requested accesses should be allowed and which should not. It acts as a filter through which all access requests made by subjects must pass. Of course the term "access" could have a meaning of either granting rights to read a document only, or to change it, or even destroy. This type of filter has come to be known as a reference monitor (Amoroso, 1994). There are numerous publications presenting research in the field e.g. (Janczewski and Low, 1998). The research concentrates mainly on the issue of how to build and run a reference monitor.
- *Technical issues related to the development of a security kernel*. The reference monitor manages the controlled access to particular information but there are numerous technical issues related to the development, implementation and running of a system in a secure way. "Secure way" means that information is protected against unauthorised access or change, and is available on request.

An analysis of the above chain of security arrangements shows a significant weak point. It is the issue of assigning security clearances to an individual. This paper presents an attempt to solve this problem by the optimisation of an information security system subject to cost constraints. As a result, an optimisation procedure that assigns formally the security clearances to all employees of an organisation has been developed. In a typical business environment this procedure is based on the position of a given person within the hierarchy of an organisation. The general principle is that "the higher you are within the company

Information Management & Computer Security
8/5 [2000] 210–217

hierarchy the highest security clearance you must have". Such an approach clearly incurs significant problems. In the one extreme a person might have a security clearance that is too high for his/her job, which increases the total cost of the security system. The higher the security clearance, the higher the cost (for instance of security training). On the opposite side a person with a security clearance too low for his/her job must obtain temporary authority for accessing specific documents. Such a procedure could be costly, time consuming and decrease the efficiency of operations. Portougal and Janczewski (1998) demonstrated in detail the consequences of the described approach in complex hierarchical structures.

A competing and more logical idea is to apply the "need to know" principle. Unfortunately, this principle does not give adequate guidance to the management as to how to set-up security clearances for each member of the staff. Amoroso (1994) describes the "principle of least privilege". The recommended application is based on subdividing the information system into certain data domains. Data domains in the main contain secret or confidential information. Users have privileges (or rights to access) to perform operations for which they have a legitimate need. "Legitimate need" for a privilege is generally based on a job function (or a role). If a privilege includes access to a domain with confidential data, then the user is assigned a corresponding security clearance. It is easy to see the main flaw of this approach is that a user has access to the whole domain even if he/she might not need a major part of it. Thus the assigned security clearance may be excessive. A similar problem arises regarding the security category of an object. A particular document (domain) could be labelled "confidential" or "top secret" even if it contains a single element of confidential (top secret) information.

In this paper we suggest another realisation of the "need to know" principle. Our method is based on the data access statements (DAS), defined for every employee as part of their job description. DAS lists all data elements needed by an employee to perform her/his duties effectively. Thus we shift the assignment of security clearance from the domain level to the element level. Figure 1 summarises existing methodologies of assigning security clearance to members of organisations.

Our approach allows not only the solving of the difficult problem of defining individual security clearances. It also connects this problem to more general problems of the security of the organisation as a whole, to the problem of security cost and cost optimisation.

In the first chapter we introduce an example of a production facility which we will use for explaining our method. In the second chapter we define the DAS being the basic measure of employee security clearance. In the next chapter we describe modelling security clearances and factors influencing this activity. In this chapter we also introduce fuzzy sets to define security clearances and show their applicability by an example. The paper concludes with a summary of the results and suggestions for future research.

A production facility example

To illustrate the problem of data security in a production environment we consider the case of a production facility. Let us assume that this facility has four managers with their responsibilities determined in the following areas: general, planning, manufacturing, purchasing and sales. Each of them is responsible for a number of activities. All this is shown in Figure 2 (after Portougal and Janczewski, 1998).

It should be noted that:

- each production unit manufactures different products;
- each organisational unit employs at least one manager;
- if a person has access to specific data but uses only part of it, it is assumed that he/she is using all of it. Therefore all data collected is used.

The production facility has an information system. Table I lists all the data elements used within this organisation. Every data element has an assigned confidentiality parameter (CP), which characterises its importance from the point of view of security. For more about assigning CPs refer to Portougal and Janczewski (1998).

In this example we assume that each data element is independent, so knowledge of a particular element does not allow one to find the value of the other. In order not to overcomplicate the example we assume all CP equal to 1.

Data access statement

There is a lot of attention in literature to employee specifications and job analysis. It is strange though, that one of the most important aspects of the job analysis, which is information use, is completely out of

specification. We suggest that in addition to the main content of a job description a data access statement (DAS) for every employee be added.

Schuler *et al.* (1992) defined the following components of a job description:

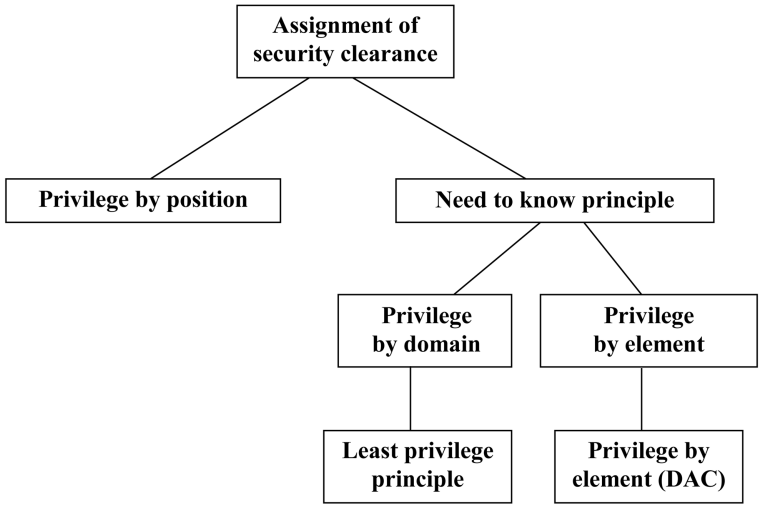
- job or payroll title;
- job number and job group to which the job belongs;
- department and/or division where the job is located;
- name of incumbent and name of job analyst;
- primary function or summary of the job;
- description of the major duties and responsibilities of the job;
- description of the skills, knowledge and abilities;
- relationship to other jobs.

The job description is the best place to define the security clearance of an employee through a DAS. It could be, for instance, an additional "bullet point" in the above list.

DAS was introduced earlier by Portougal and Janczewski (1998), and was defined as follows:

- DAS of a staff member is a vector, containing data access statements elements (DASE) as its components.
- Each DASE defines what type of access to information/data is allowed (read, write, delete, etc.).
- Each DASE is defined as a result of the analysis of the job description document related to the given position.
- Each DASE has a confidentiality parameter CP assigned (being an element of the organisation's database it should have the same value (CP), e.g. from Table I).

Figure 1
Taxonomy of assigning security clearances methods



DAS statements for the facility presented in Figure 2 are shown in Table II. The row numbers indicate corresponding DASE, like "1" denotes the volume of production. At the bottom of the column the total value of information accessible is shown. We shall call it SCV – security clearance value, thus tying the assignment of a security clearance to the volume of accessible information.

Modelling security clearances

The security clearance allows a person to access a certain part of a database. We can assume that the optimum security clearance is assigned strictly in accordance with the "need to know" principle. Unfortunately, the "need to know" principle assigns to every employee a specific area of the database, and generally there will be as many different areas as the number of employees. At the same time, there is always a limited (two-four) number of security clearances. Thus the assigned clearance will practically always be different from optimum, below or above that optimal point.

Clearly, the probability of an information leak goes up, when the difference between the actually assigned clearance and the optimum clearance is increasing. At the same time assigning extra security clearance involves extra cost. Let us analyse the cost of assigning security clearances to particular persons in a more detailed way.

The best known security standard, British Code of Practice (BS 7799, 1995) introduces ten categories of security measures divided into such domains as:

- management of information security;
- security of the physical site;
- computer and network security;
- access control;
- system development and maintenance;
- personnel security;
- business contingency planning.

It is obvious that there is a positive correlation between security of the system, numbers of security measures, and their costs, i.e.:

more security measures $\Longrightarrow$ more secure system $\Longrightarrow$ more costs

Many sources (Frank, 1992) indicate the above correlation is not linear but has a tendency to grow exponentially. Similar situations exist in the case of assigning security clearances. The higher security clearance of an employee means a higher expenditure to the employer. The structure of costs would be somehow different from the

Figure 2
Organisational structure of the facility

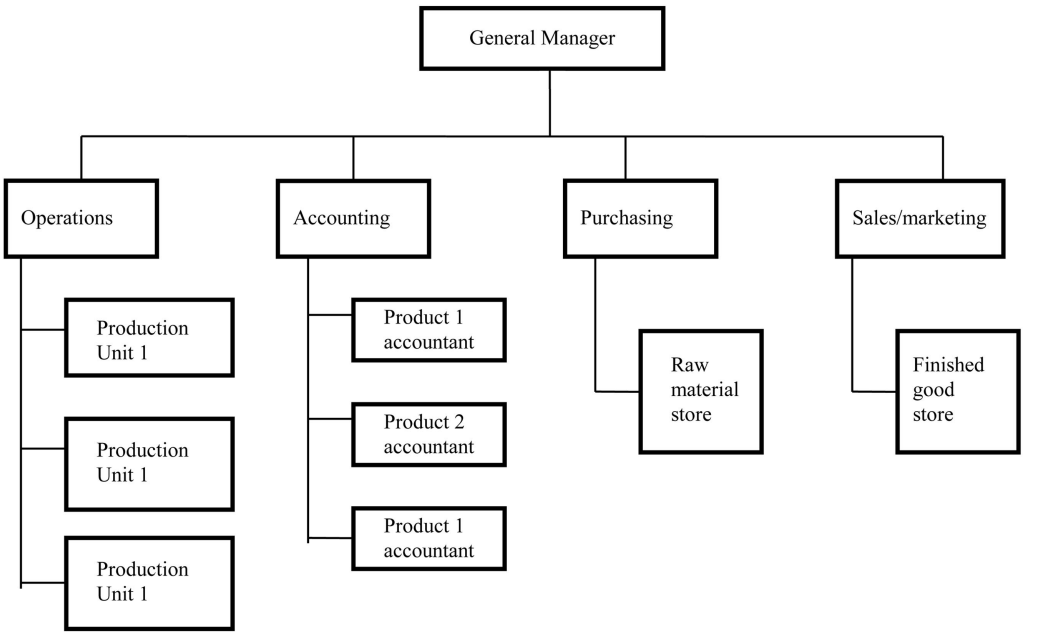


Table I
Database elements listing

Database elements	CP
1 Volume of products	1
2 Sales	1
3 Labour cost	1
4 Material cost	1
5 Cost	1
6 Labour cost (of N)	1
7 Materials cost (of N)	1
8 Sales (by products)	1
9 Volume of products (by product)	1
10 Cost (by products)	1
11 Costs (materials)	1

Table II
DAS for all employees of the production facility

	GM	OP	AG	PUR	S&M	PUN	ANM	RM	FGS
1	√	√	√		√				√
2	√		√		√				√
3	√	√	√						
4	√	√	√	√				√	
5	√	√	√		√				
6	√	√	√			√	√		
7	√	√	√	√		√	√	√	
8	√		√		√	√	√		√
9	√	√	√		√	√	√		√
10	√	√	√			√	√		
11	√	√	√	√		√	√	√	
Total (SCV)	11	9	11	3	5	6	6	3	4

Notes: GM = general manager; OP = operations; AG = accountant general; PUR = purchasing; S&M = sales and marketing; PUN = production unit N; ANM = account N manager; RM = raw material store manager; FGS = finished goods store

security measures listed above. The costs like those listed below would be of significance:

- examination of candidate credentials;
- security training;
- security equipment (especially for accessing protected zones, either physical or system);
- management of the system controlling the security clearances.

Again one might expect that there is a correlation of security clearances with costs:

higher security clearance granted $\Longrightarrow$ higher costs for the organisation

The security clearances should be directly related to the jobs and should follow the "need to know" principle. The 5th Principle of the *Guidelines for the Security of Information Systems* prepared by the OECD recommends that "Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems" (OECD, 1992). The OECD proportionality principle states that to operate in an effective mode an organisation must match security clearances of their staff with the job profiles very carefully.

The security clearances are designed to subdivide the employees of the organisation into classes according to data access privileges, e.g. secret, confidential and

general. Following the usual approach, borderlines should be drawn, defining the minimum amounts and importance of data in use for each category. It was analysed in the Introduction that, before our development of quantitative measures of confidentiality (CP), this subdivision was performed either by employees' position or by assigning security categories to data domains, and then using these categories for defining clearances. With the CP and SCV defined the problem becomes much easier and more logical to solve.

In our example (Figure 3), let us have three security categories: general, confidential and secret. We shall define the borderline SCV between general and confidential as four, and the borderline SCV between confidential and secret as eight. If the total SCV of information in use by an employee is less or equal to four, then this person is not required to follow special security procedures at all, and he/she would be assigned a general clearance. If the total SCV is between five and eight, then the confidential clearance should be applied, meaning that this employee is under an obligation to use and follow all the security procedures defined for this clearance. Similarly, if the SCV of data in use is more than eight, then this employee should be assigned the secret clearance.

Though this procedure is simple and easy to understand, nevertheless it has two weak points:

1 This procedure implies that the security experts will be able to define the borderlines. In reality it is not so easy, and sometimes the decision about the borderlines is provided by reasons well outside the model, for example by position.
2 Under this procedure it is hard to explain why employees with SCV close to the borderline from different sides have different clearances. What is the crucial reason for an employee with SCV equal to 0.79 to have a clearance confidential, but his/her colleague with SCV = 0.81 to have secret clearance?

Both points indicate an inadequacy in our security clearance modelling. Basically, the inadequacy comes from using a classical crisp set for modelling, like this used by (Pfleeger, 1997). The crisp set is defined in such a way as to dichotomise the individuals into two groups: members (those that certainly belong to the set) and non-members (those that certainly do not). A sharp distinction should exist between members and non-members of the class. This is definitely not so in our case. The classes of security clearances do not exhibit this characteristic. Instead, the transition from member to non-member of one class appears gradually rather than abruptly. This is the basic concept of fuzzy sets.

In the first fuzzy model we shall assume only two security clearance classes: general (set G) with no security cost and secret (set S) with a security cost A for each member of the class. The membership functions of class S are given in Figure 4. The vertical lines on Figure 4 represent the employees of the example company and the value of their membership function in the set S. General manager and accountant general have the value equal to 11, operations manager has it equal to 9/11, purchasing manager has it equal to 3/11, etc.

If we assign to every manager the security clearance secret, then the cost of the security system will be equal to 9A (as there are nine managerial positions in the company). If this is not affordable, then some of the managers will be put into G class. This involves a risk of information leak.

Let us assume that this risk is proportional to SCV (the more a person knows the higher is the risk). We shall introduce the risk factor (RF) for an employee i as:

$$\mathrm{RF}_i = \mathrm{SCV}_i/\mathrm{SCV}_{max}$$

A good estimate for the company risk factor (CRF) would be either:

$$\mathrm{CRF}_{max} = \max_i \mathrm{RF}_i,$$

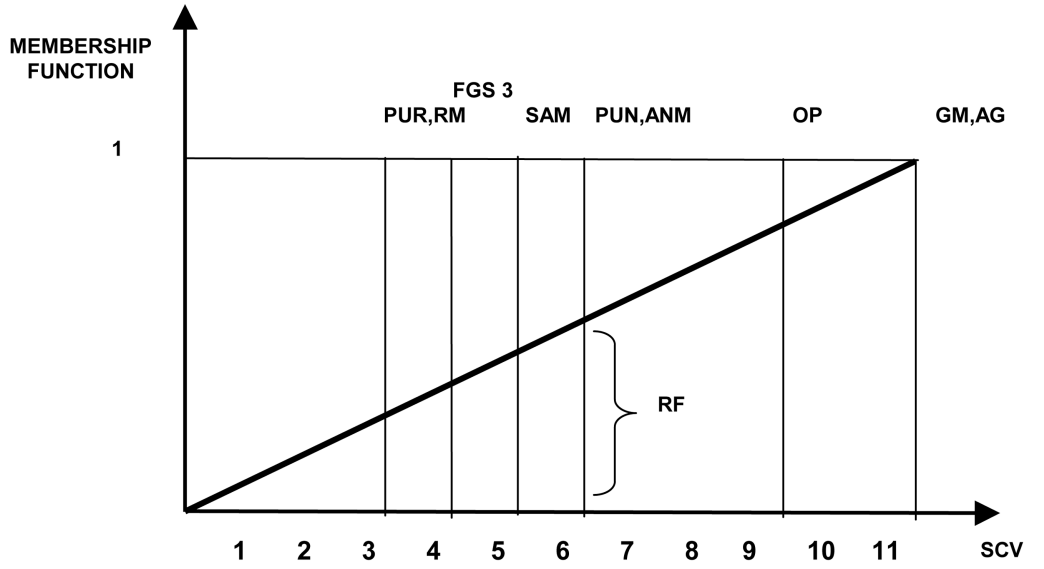
or

$$\mathrm{CRF}_{av} = \Sigma_i \mathrm{RF}_i/\mathrm{N},$$

Figure 3
Security categories (crisp representations)

Information Management & Computer Security
8/5 [2000] 210–217

Figure 4
Membership function for the fuzzy set "secret"



where N is the total number of employees. CRF_{max} characterises the risk of information leak from the most informed employee. It is better for evaluation than CRF_{av}, when the SCV_i of the employees are diverse. Sometimes both are useful.

The risk factor can not be used directly for the evaluation of real security threats. It is only a coefficient in a more complex equation with unknown chances of a breach of security and losses from it. But the assumption of its proportional value to the security risk gives it a good comparative meaning.

Let our example postulate that the company has a security budget of 3A, or that it can afford to assign the secret clearance only to three employees: GM, AG and OP. The security risk factors will be:

$$CRF_{av} = (3 + 3 + 4 + 5 + 6 + 6 + 0 + 0 + 0)/11/9 = 27/99.$$

$$CRF_{max} = 6/11$$

If we increase the security spend to 4A (33 per cent increase, one more person classified as S), then the CRF_{av} will drop to 21/99 (22 per cent decrease), but CRF_{max} would not change. It is worth thinking whether to increase the security spend or not in this situation. Thus, the main benefit of the CRF is the possibility to use it for comparing different assignments of security clearances.

Although the two classes model is too simplistic, nevertheless it shows the main problem of a security system design. The problem is that practically no organisation can afford a security system with a zero risk factor, and it is forced to look for a suitable trade-off between the cost and the risk factor.

We shall show that introduction of intermediate classes helps in security improvement without cost increases.

Let us introduce an intermediate clearance confidential (set C). We shall assume that the security procedures designed for this clearance eliminate the risk of data leakage for all employees with SCV_i no more than 4. Let the cost of these procedures be B = A/3, and the security budget as before is 3A. The possible variant of assigning clearances to employees is shown in Figure 5. In this variant we sacrifice the clearance S for the operations manager (OP), changing it to C, which incurs a security risk factor of (9 – 4)/11. It allows the provision, within the limits of our budget, of two more employees with higher risk factors, PUN and ANM, with the same clearance C. This will decrease their risk factors by 4/11 each.

The security risk factors will be:

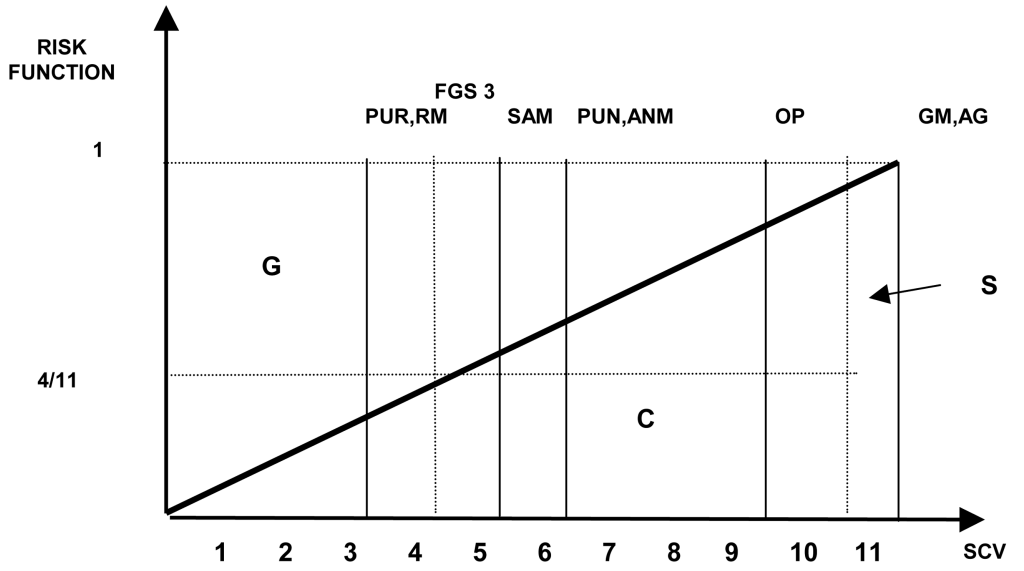
$$CRF_{av} = (3 + 3 + 4 + 5 + 2 + 2 + 5 + 0 + 0)/11/9 = 24/99.$$

$$CRF_{max} = 5/11.$$

This shows a significant improvement in security estimates.

The next step will be to sacrifice the S clearance of either GM or AG and to provide C clearances for him/her and additional two employees with higher risk factors. This will leave only two persons in the G class; six persons will be in the C class, two of them having a non-zero risk factor.
The security risk factors for this distribution show the following improvement:

Figure 5
Risk function and its cover by three classes G, C and S



$$CRF_{av} = (3+3+0+1+2+2+5+6+0)/11/9 = 22/99.$$
$$CRF_{max} = 6/11.$$

The first criterion has decreased, but the second shows an increase. We can choose either the previous variant of clearances distribution if we prefer the second criterion, or to go further on if we prefer the first one. Then the final logical step is to use the budget for assigning all employees a uniform clearance C. In our case this does not show further improvement. Generally, an analysis of both company risk factor functions CRF_{av} and CRF_{max} show the best way for their optimisation, but this analysis is outside the scope of this paper.

Security modelling for data elements with different confidentiality parameters

One of the assumptions of the described model is that CP is equal for all the data elements. This assumption restricts the area of this model implementation to the companies that consider all data elements equally important. In most cases, the data elements are conceptually not homogeneous from the confidentiality point of view. It is not very difficult to accommodate this. Portougal and Janczewski (1998) suggested an expert evaluation procedure that helps to establish real values of CP from the point of view of security experts.

The method of calculating CRF_{av} and CRF_{max} stays the same but DASE would have different values thus shifting the position of an individual along the horizontal axis (Figure 3).

Conclusion

The main results of this paper may be summarised as follows:

- For the full and complete implementation of the "need-to-know" principle we introduced data access statements (DAS) as part of an employee's work description. Thus the access to the information is granted to every employee on the data element level as opposed to the existing practice of granting access on a domain level.
- We suggest changing the existing practice of assigning security categories to data base domains, and to assign instead a confidentiality parameter (CP) to every element of the database. The database will be characterised from the confidentiality point of view in more detail.
- We showed that current crisp models of assigning security clearances do not include cost and efficiency optimisation. Instead we developed optimisation models, based on fuzzy sets theory.
- As a measure of efficiency of the security system we introduced the company risk factor (CRF), which makes it possible to compare different ways of security organisation under a limited budget.

Further research in this direction might include the development of optimisation models, based on analysis of both company risk factor functions CRF_{av} and CRF_{max} and

Information Management & Computer Security
8/5 [2000] 210–217

the structure of the set of feasible solutions. Another direction of research includes the development of models optimising costs of the security system under risk constraints.

References

Amoroso, E. (1994), *Fundamentals of Computer Security Technology*, Prentice-Hall, Englewood Cliffs, NJ.

British Standard BS 7799 (1995), *Code of Practice for Information Security Management*, UK.

Forcht, K. (1994), *Computer Security Management*, Boyd & Fraser Publishing Company, USA.

Frank, L. (1992), *EDP-Security*, Elsevier Science Publishers, The Netherlands.

Janczewski, L. and Low, B. (1998), "Reference monitor for hypermedia-based hospital information systems", in Papp and Posch, G. (Eds), *Global IT Security*, Österreichische Computer Gesellschaft, Austria.

Jordan, E. (1999), "Business and computer contingency planning in Australia", *JBC – Continuity*, Mcquarie Report, Summer 98 issue, Australia.

Leung, V. (1998), "Optmization of information security policy development", MCom. Thesis, Department of MSIS, The University of Auckland, New Zealand.

OECD (1992), *Information Computer Communications Policy, Guidelines for the Security of Information Systems*, Publication No OECD/GD (92) 190, France.

Pfleeger, C. (1997), *Security in Computing*, Prentice-Hall, Englewood Cliffs, NJ.

Portougal, V. and Janczewski, L. (1998), "Industrial information-weight security models", *Information Management & Computer Security*, Vol. 6 No. 5.

Schuler, R. *et al.* (1992), *Human Resource Management in Australia*, Harper Educational, Australia.