29

A Day in the Life of a Swedish IT Security Officer: An Attempt at an Empirical Study

Stewart Kowalski Ph.D.
Centre for Security Informatics,
Stockholm University & Royal Institute of Technology
Electrum 230, 164 40 Kista Sweden, e-mail : stewart@dsv.su.se*

ABSTRACT

This paper describes an attempt to collect data on the day-to-day activities of IT security officers in Sweden. A number of different techniques for collecting data are discussed including, analysis of employment adds for IT-security officers, job descriptions, mail-in questionnaires and interviews. The results of interviews with 10 IT security officers are presented. The interviews indicated that a large portion of the IT-security officer's day (20-30%) is involved with education and awareness training of personnel. Few of the officers interviewed (two) actually performed operational security matters and most were involved with coordination of security activities within operational units. All interviewed indicated that they see their task as being more social than technical oriented and indicated that their day-to-day decisions are based more on hunch and intuition than in-depth analysis.

1. INTRODUCTION

From a pure micro-economic perspective the IT security officer is one of the most costly security measures that organisations use to protect themselves against IT crime. A survey done by the Electronic Trends Publication [1] on American companies indicated that 68% of the expenditures for IT security[1] are personnel cost. Surprisingly, even though the IT security personnel function is the most expensive measure, very little research has been done to analyse its effectiveness. Those studies that have been done indicate that as little as 8% of the reported unauthorised access made in IT systems are detected by IT security personnel and as much as 32 % are detected by pure accident [2] . While the validity and relevance of these statistics, as most statistics in the security field, can be questioned, they do suggest that more research on the relationship between the activity of IT security personnel and the effectiveness to detect and deter IT crime and abuse needs to be performed. This paper describes an attempt to perform a study of the activities, roles and functions of IT security officers in Swedish organisations.

---

* Present address, Telia Research AB, Systems Research Information Security
136 80 Haninge, Sweden, e-mail :stewart.kowalski@haninge.telia.se

[1]In Beer's report of Electronic Trends Publication study the term used was computer, not IT personnel.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

1.1. Outline of the Paper

In section two of the paper the background of the study is presented and the problems of collecting empirical data on day-to-day activities of IT-Security Officers is examed. Different methods used to collect data are discussed. Preliminary findings from the questionnaires and interviews are also presented. Section three concludes the paper with a general discussion of the need for more empirical studies in the area of IT security and makes suggestions for future work.

2. THE STUDY

2.1. Background

In the spring of 1993 as part of a doctoral program in IT security at the Royal Institute of Technology [3] a project group[2] was formed to collect data on IT security officer's day-to-day activities. Like other studies done on security professionals, [4,5], it was hoped that this data would debunk many of the myths of IT security work and set a more firm scientific foundation for the introduction of effective IT crime prevention activities.

The difficulties in collecting data on activities of security professionals are well documented [5]. There are a number of theoretical and practical problems. First theoretically, empirical data can only be generated by, unbiased study, observation and isolation of a repeatable and/or reproducible natural and social phenomenon. However given the complex relationship of the IT security problem to technology and social change it is extremely difficult to isolate and almost impossible to repeat IT security relevant events and activities. Practically, like soldiers in war, security professionals spend most of their time waiting and preparing for something to happen. Thus even if one is granted the permission to observe them in action, which is the best way to obtain unbiased information on their activities, one has to spend a great deal of time watching them "shine their boots" and fraternise.

A number of different methods for collecting data were considered for the study. Participation observation while being the best method to obtain unbiased information turned out to be impractical since it was difficult to obtain subjects that would agree to be monitored. A diary system where an IT security officer would note his or her activities was also considered but this method had to be dropped when only a few IT officer's volunteered. It was decided finally to use as series of methods where the data collected with one method could be used to refine the process of the next method.

Following a brief literature search of job descriptions for IT security officers a content analysis of employment adds for IT security officers over the period 1988-1992 was performed. The data from the content analysis was used to construct interview protocols and 10 interviews of IT security officers were performed. The results of the interviews were used to construct a mail-in questionnaires which were then distributed to the approximately 750 members of the Swedish

---

[2]The author would like to acknowledge the members of the group, Anders Holmbjörn and Jan Weideskog and also give special thanks to Walter Holmer, Staffan Jackson and Bengt Angerfelt for assisting the group.

Information Processing Society Special Interest Group for Security (SIG/SEC). In the next section these methods will be discussed in detail.

2.2. Literature Search

A problem that arouse when performing the literature study of IT security officer's job descriptions was that there exist no standard nomenclature for job titles within the IT security area. The most common title found was "ADB-sähertschef" which can be translated into English as EDP security manager. However a number of titles were used such as, EDP security administrator, Computer Security Co-ordinator and Data Security Supervisors to include only a few. To deal with this problem it was decided that for this study the term IT security officer would refer to all job functions directed involved with management, operation and co-ordination of IT security functions.

A number of different references were found in the Swedish literature where job descriptions for IT security officers are proposed and discussed. These sources ranged from material published by the Swedish parliament [6] to pamphlets distributed by a consortium[3] of Swedish Data Process White Collar Unions [7]. In 1990 a comprehensive report of the roles and responsibilities for IT security in Swedish organisations was published by the Ministry of Public Administration [8]. In this report a number of job descriptions for IT security officers are suggested. Below is a translated version of an example of such a job description:

It is the responsiblity of the information security officer to follow the directives issued by upper management and:

- be responsible for the co-ordination of all information security work in the organisation
- ensure that established of an upper management defined information security policies by issuing guidelines
- ensure that existing laws, recommendations and directions affecting information security are followed
- develop suggestions for rules and directions for the information security activities in the organisation
- ensure that system development, EDP operation and maintenance of the EDP system is done with respect to existing requirements of information security
- initiate and perform information security analysis
- check access control system
- give advice and support in information security issues in the organisation
- ensure that the information security are followed up according to established regulations by top management
- ensure that affected personnel receive necessary education and information within the area of information security
- keep top management informed about the status of information security in the organisation.

---

[3] SIF, SBmf FTF. It is of interest to note that preliminary survery result of this study indicate that 80% of IT-security officers in Sweden belong to white collar unions.

2.3. Analysis of Employment Adds

Due to limited resources in the project only one Swedish newspaper, Computer Sweden, [9] was scanned. The employment adds for security workers related to the computer field from 1988- 1992 were collected. Unofficial estimates by the staff of the paper[4] place employment adds in this weekly paper, which had a circulation of approximately 50,000, at about 200-400 a year. Of these 200-400 adds only 1 or 2 percent of the adds were for employment of IT security officers. It should be noted however that this is a rough estimate since there is very little agreement on the terminology used to describe computer professional job titles. A clear trend in the employment adds however was that the area of security was included more and more as part of job descriptions of other computer professionals. Thus an add for a PC coordinator had PC security as an area of responsibility. Table 1 shows a breakdown of the adds by year. Column 1 indicates adds which specifically had security in the job title while column 2 indicates the adds which had security activities as part of the job description.

Table 1

Security Related Employment Adds Computer Sweden 1988-1992

Year	Job Title Included IT-Security	Job Description Included IT-Security
1988	6	0
1989	3	2
1990	3	2
1991	3	6
1992	2	7

Although the numbers are too few to draw any conclusions it appears that security activities within organisations in Sweden are becoming less and less specialised function and more and more a part of normal operational activities.

[4]Interview with Åke Bowman, November 1992.

2.4. Interviews

With the data collected from the literature search and the content analysis of the employment adds an interview protocol was constructed. There were 65 questions in the interview protocol which took approximately 2-3 hours to complete. Ten IT security officers were selected and questioned about their day-to-day activities. The significant findings from the interviews will be presented here.

A number of questions in the interview focused on the daily contact an IT security officer had with co-workers. Specifically, they were asked to rank the following methods for co-ordination according to importance and time spent. Table 2 shows the results of the ranking.

Table 2
What means do you use to co-ordinate security activities?

Activities	Rank Order	Percentage of Time
Informal Contacts	1	20
Security Communities	3	20
Conferences	5	5
Telephone Contact	2	15
e-mail	-	-
Memo	4	10
Seminar	6	30

Thus it appears that management by walking around occupies a large part of an IT security officer's day. Also it appears that e-mail was at least in 1993 not a method that these IT security officers saw as an effective coordination tool.

When IT security officers are not walking around they appear to be spending most of their time informing or educating. When asked how much of their time is taken up with educating and informing personnel the response was between 30-50 percent with the average response being 40 percent.

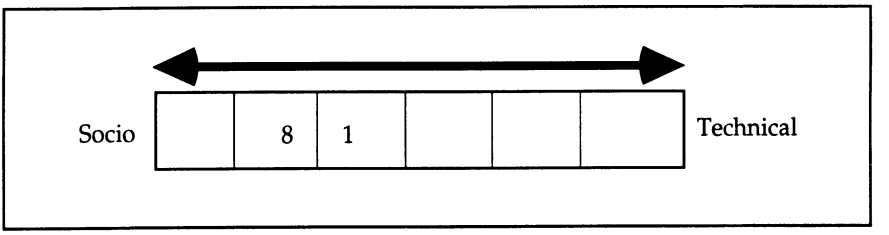
Very little of the security officer's time was taken up with actively checking the security operations. None dealt with distribution and password management and only two actually said that they had performed spot checks on the system in the last year and most stated that these types of activities were the responsibility of the line mangers.

The average age of the officers surveyed was 45 years. There was a large spread in their anual income, the lowest being 240,000 Swedish Crowns and the highest being close to 400,000 Swedish Crowns. To put this figure into perspective for an international audience, of the 3,5 million male workers in Sweden in 1990 only 700,000 had an anual income over 200,000 Swedish Crowns [10].

The ten security officers were asked to classify their job on two scales. The first scale was a social technical continuum. There is a constant debate within the IT security officer community in Sweden as to whether the job function is more technically oriented or more socially oriented.

Figure 1

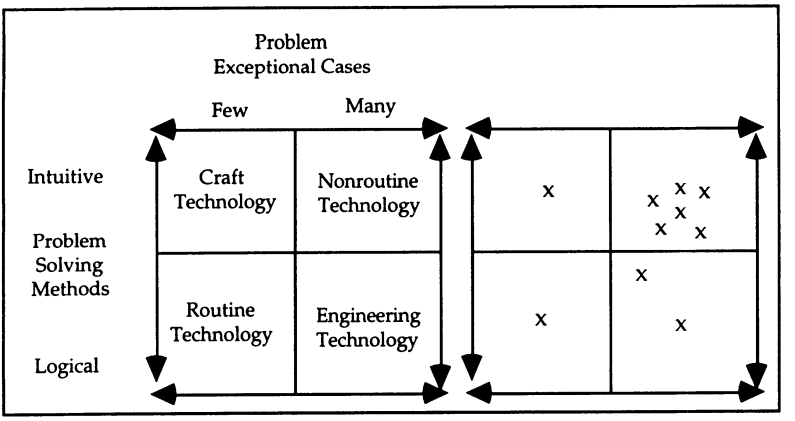
Where would you place IT security work on this Socio-technical Continuum?



As can be seen from the Figure 1 most[5] of the IT security work is seen as being more social than technical.

The respondents were also asked to place IT security work activities in the Perrow's technology type dichotomy of exceptions vs. search.

Figure 2
Indicate with an X where you believe security work is best classified in Perrow's dichotomy.



Thus it appears, at least among the IT security officers interviewed, that intuitive skills are valuved high. This could explain why informal contacts, in Table 2, are ranked as one of the most important activities for co-ordinating security in their organisation.

---

[5]One respondent did not answer the question because he did not believe that a continuum of socio and technical was a valid representation of the problem.

2.5. Mail-in Questionnaire

After considering the results from the literature search, content analysis of employment adds and the interviews it was decided to construct two questionnaires. One questionnaire focused on the job descriptions and titles of IT security officers in Sweden while the other questionnaire was concerned with day-to-day activities of IT security officers. The questionnaires were mailed to the 750 members of the Swedish Information Processing Society Special Interest Group on Security SIG/SEC. Half of the members received the job description questionnaire while the other half received the daily activity questionnaire. The response rate to the questionnaire was over 50 % with more than 400 questionnaires returned. At the time of writing this paper the statistical data from the questionnaires is still being compiled[6] and due to the changes in the delivery date for the paper only the preliminary results on the activity questionnaire can be presented here.

2.5.1 Preliminary Results from the Questionnaires

The designed philosophy for the activity questionnaire was to make it a structured diary format. A number of different possible work activities for an IT security officer were listed[7] and the respondents were requested to check off which activity was performed that day the questionnaire was filled in. As Robinson [12] points out there are a number of validation problems with this form of data collection but it was believed that with a 50 percentage or more response rate these problems can be addressed. Preliminary tabulation of the results of the survey indicates that the greater part of an IT security officer's day is administrative in nature. Co-ordination of policy development and security awareness training of staff are the most common day-to-day activities. Very little activity is operational in nature, that is to say, few IT security officers were involved with actively checking audit logs and investigating incidents. Only 30 per cent of the respondents had worked with access control functions and only 20 per cent had worked with active monitoring functions.

3. CONCLUSIONS

To the author's knowledge this study is the first attempt to collecte data on the day-to-day activities of IT security officers. There are a number of theoretical and practical problems which need to be addressed before future work should be undertaken. First, a nomenclature for IT security workers and managers needs to be established. Without an established nomenclature it will be impossible to collect empirical data and there will be a tendency to rely on anecdotal data. Second, a number of different data collection methods need to be experimented with in order to determine the most efficient for IT security officer studies. Finally and most important, the IT security community needs to establish more critical self reflecting attitudes to it role and function in modern organisations.

---

[6]Those interested in obtaining the results of the survey can contact me via my e-mail address.

[7]For an English translation of the activity questionnaire see appendix.

References

[1] Johan Beer, "Nyheter från Världen", Computer Sweden, Aug. 24th., 1990.

[2] Johan Beer, "Nyheter från Världen", Computer Sweden, 1990.

[3] Stewart Kowalski, IT-insecurity: A Multi-disciplinary Inquiry, Doctoral Thesis, Royal Institute of Technology, Stockholm Sweden, 1994.

[4] Reiss A., Jr. "The Police and the Public", New Haven, Conn.: Yale University Press, 1971.

[5] Banton, M., The Policeman in the Community, London, Tavistock, 1964.

[6] Riksdagen förvaltningskontor, ADB-säkerhet i riksdagen, June 1992.

[7] DataForum, SIF, SBmf, FTF, Yrke för data-folk, Nov. 1992.

[8] Civildepartementet, SAMS rapport Ds 1990:43, De verksamhetsanvarigas säkerhetsansvar, May 1990.

[9] Computer Sweden, CW/Communication AB, Sweden.

[10] Statistics Sweden, Sweden in Figures, March 1993.

[11] Perrow Charles, A Framework for Comparative Analysis of Organizations, American Sociological Review, 32 (April 1967): 194-208.

[12] Robinson, J., The Validity and Reliability of Diaries versus Alternative Time Use Measures, Juster & Stafford, 1985.

Appendix 1
Translated Activity Questionnaire

	Introduction			
	Are you professionally active in the area of information IT-security?	1	( )	Yes, as an employee.
		2	( )	Yes, as an external consultant.
	(300)	3	( )	No - start with question **38**

A number of different possible activities for an EDP/Information security officer are listed below. The activities are divided into different organisational levels. Indicate which of the activity you performed yesterday. The goal of the survey is to come to a better understanding of a typical working day for an EDP/Information security officer.

	Question 1-11 are related to work activities at the organisation level	Did yester-day	Did Not do yester-day	Not within work area
1	Worked with co-ordination of information security activities at the organisation level.	( )	( )	( )
2	Worked with developing information security policy for the organisation as a whole.	( )	( )	( )
3	Verified that established organisational information security policy was being followed.	( )	( )	( )
4	Verified that established organisational information security procedures and rules were being followed.	( )	( )	( )
5	Worked with the development of organisational rules, procedures and guidelines for information security.	( )	( )	( )
6	Performed spot checks, test transactions, as to adequate functioning of EDP security systems.	( )	( )	( )
7	Initiated/performed risk and threat analysis of the information security for the organisation.	( )	( )	( )
8	Worked with the organisation's EDP access control system.	( )	( )	( )
9	Reported, to top management, the information security status of the organisation.	( )	( )	( )
10	Worked with evaluation/certification of EDP security products (backup program, virus programs etc.) at the organisational level.	( )	( )	( )
11	Worked with evaluation/certification of no related EDP security products (fire theft, backup power etc.) at the organisational level.	( )	( )	( )

Question 12-22 are related to activities at the <u>division level</u> of the organisation.	Did yester-day	Did Not do yester-day	Not within work area
12 Worked with co-ordination of information security activities at the division level.	()	()	()
13 Worked with the development of information security policy for the division.	()	()	()
14 Verified that established information security policy was being followed in the division.	()	()	()
15 Verified that established division information security procedures and rules were being followed.	()	()	()
16 Worked with the development of the organisation's rules, procedures and guidelines for information security at the division level.	()	()	()
17 Performed spot checks, test transactions, as to adequate functioning of EDP security systems.	()	()	()
18 Initiated/performed risk and threat analysis of the information security for the division.	()	()	()
19 Worked with the division's EDP access control system.	()	()	()
20 Informed/educated staff at the division level on information security issues	()	()	()
21 Worked with evaluation/certification of EDP security products (Backup program, virus programs etc.) at the division level.	()	()	()
22 Worked evaluation/certification of no related EDP security products (fire theft, backup power etc.) at the division level.	()	()	()

	Question 23-33 activities at the section level of the organisation.	Did yester-day	Did Not do yester-day	Not within work area
23	Worked with co-ordination of information security activities at the section level.	()	()	()
24	Worked with the development of information security policy for the section.	()	()	()
25	Verified that established organisational information security policy was being followed in the section.	()	()	()
26	Verified that established organisational information security procedures and rules were being followed.	()	()	()
27	Worked with the development of section specific procedures and guidelines for information security.	()	()	()
28	Performed spot checks, test transactions, as to adequate functioning of EDP security systems.	()	()	()
29	Initiated/performed risk and threat analysis of the information security status of the section.	()	()	()
30	Working with the sections EDP access control system.	()	()	()
31	Informed/educated personal in the section, on the information security issues within the section.	()	()	()
32	Worked with evaluation/certification of EDP security products (Backup program, virus programs etc.) at the section level.	()	()	()
33	Worked evaluation/certification of no related EDP security products (fire theft, backup power etc.) at the section level.	()	()	()

	Other activities:	Did yester-day	Did Not do yester-day
34	Attended internal company courses.	()	()
35	Attended external courses.	()	()
36	Attended internal section meeting.	()	()
37	Attended external conference.	()	()

Background information:

	Title/Position?	(338) 1 Security Officer	2 EDP security officer	3 Infosec Officer	4 Infosec Co-ordinator	5 Infosec Responsible	
		6 Other					
39	How do you think your position should be titled?	(339) 1 Security Officer	2 EDP security officer	3 Infosec Officer	4 Infosec Co-ordinator	5 Infosec Responsible	
		6 Other					
40	Do you work with security full-time in your position or part time?			-25%	26-50%	51-75%	76-100%
41	Sex?					Male	Female
42	How many years of experience do you have working with security?			Less than1 year	1-5 years	5-10 years	More than 10 years
43	How many employees are there in your organisation?	1-5	6-30	31-100	101-500	501-1000	1001-
44	Which age group do you belong to?	-25	26-35	36-45	46-55	56-65	66-
45	How do you keep informed about developments in information security?	Literature	Col-leagues	Conf-erences	Govern-ment	News-papers	Others
46	Education background Indicate the highest completed level	Elementary Junior High	High school	College	University	Post-graduate	Others
47	In what industrial sector is your organisation/work area?	(347) 1 Bank/insurance/ finance	2 Public Sector	3 Manufacturing	4 Service sector	5 Health Care	6 Others