Assessment of Enterprise Information Security - The Importance of Information Search Cost –

Erik Johansson, Mathias Ekstedt, Pontus Johnson
Department of Industrial Information and Control Systems
Royal Institute of Technology (KTH)
erjo@ics.kth.se

Abstract

There are today several methods and standards available for assessment of the level of information security in an enterprise. A problem with these assessment methods is that they neither provide an indication of the amount of effort required to obtain the assessment nor an approximation of this measure's credibility. This paper describes a part of a new method for assessing the level of enterprise information security expresses the credibility of the results in terms of confidence levels and make use of an estimation of the cost of searching for security evidence. Such methods for predicting information search cost of assessments are detailed in the paper. Search cost predictions are used for providing guidance on how to minimize the effort spent on performing enterprise information security assessments. The conclusions are based on a security assessment performed at a large European energy company and a statistical survey among Swedish security experts.

1. Background to research

This paper presents results from an ongoing research project that focuses on the development of a method for the assessment of *Enterprise Information Security*. The project is part of a comprehensive research program, the *Enterprise Architecture Research Programme* (EARP) that exploits the discipline of *Enterprise Architecture* as an approach for managing the company's total information system portfolio. The primary stakeholder of the Enterprise Architecture is the *Chief Information Officer* (CIO) who is responsible for the management and evolution of the enterprise system – i.e. the overall system of IT related entities. The overall goal of the research program is to provide the CIO function with architecture-based tools and methods for planning and decision making with regard to enterprise-wide information systems [8].

Information is an important business asset in an enterprise. Hence *enterprise information security* has become an increasingly important system quality that must be carefully managed. Although enterprise information security is one of the most central areas for enterprise IT management, the topic still lacks adequate support for decision making on top-management level [7]. Good decisions require good information. Credible information does however not come for free. Information needed for the assessment can be more or less easy to find within the organization, so the benefit of well-informed decision support in terms of an Enterprise Information Security assessment must be traded for its cost. Consequently, a credible and efficient method for assessing the current state of Enterprise Information Security would be desirable [3].

1.1. Purpose and Scope

The purpose of the overall research project is to develop a method for the assessment of Enterprise Information Security (herein denoted as the EIS method).

In order to determine the assessment objectives unambiguously, the area of enterprise information security (EIS) was in a previous paper defined in terms of a tree structure [9]. In a later paper [10], that structure was prioritized to reflect the relative importance of the different aspects of enterprise information security. This prioritization has two purposes, it further clarifies the assessment scope and it is used in order to minimize the assessment cost. In a third paper [11], the credibility of the assessment results is addressed with a statistical approach combined with ideas from historical research and witness interrogation psychology [2].

In this paper, the concept of *information search cost* is addressed in order to increase the cost-effectiveness of the method. This paper promotes the principle *"Don't*

0-7695-2507-5/06/$20.00 (C) 2006 IEEE

www.manaraa.com

look for what you cannot (afford to) find!" Two different information search cost prediction methods are presented.

1.2. Outline

The next section presents an overview of the EIS method as a whole. Section 3 introduces the concept of information search cost and discusses its importance for the overall cost and credibility of the assessment results. Section 4 details the two prediction methods for assessment cost. In section 5 the benefits of using these methods in EIS assessment is being presented. Section 6 concludes the paper.

2. Presentation of the EIS Method

In this section the fundamental ideas behind the EIS method are introduced. The purpose of the EIS method is to perform an assessment of the overall enterprise information security at a given company. There are some important requirements that separate this security assessment method from others. Firstly, the assessment result is to be presented as a *single value* on a scale, e.g. a percentage score. Secondly, an explicit requirement on the method is that the *credibility* of the assessment score is presented. Thirdly, the assessment procedure should be as *cost-effective* as possible. In particular, this relates to the cost of searching for information in the company under review.

The following subsections discuss the definition of the enterprise information security area and how a very simple ternary score may be refined into a useful percentage score. It details the main costs in presenting such a score with a high credibility and presents a simple method for assessment of the EIS score, providing both a score and the credibility of that score. Finally, a more elaborate method is proposed, where cost-effectiveness is explicitly taken into account.

2.1. A Ternary Score for Enterprise Information Security

When attempting to assess *Enterprise Information Security* (EIS), the first problem encountered is what is to be assessed; what exactly is the area of inquiry? The natural answer is to rely on established knowledge in terms of literature on the subject. When searching the available literature on information security aspect related to the enterprise-level, however, this turns out to be a wide and oftentimes contradictory collection of books, reports and papers. The arguably most well-established sources related to enterprise information security are documents from international and national standards on the topic. It would be desirable to use these as a foundation in an evaluation of the level of enterprise information security. If a company satisfied all standards, it would arguably have a very high degree of enterprise information security. In this work the *ISO/IEC 17799 Code of Practice for Information Security Management, NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems*, *The Standard of Good Practice for Information Security*, and the *OCTAVE® Catalog of Practices* have been used [1][4][6][13]. These highly cited standards within the area have been compiled into a database of questions (i.e. the requirements in the standards have been rephrased into questions), cf. Figure 1.

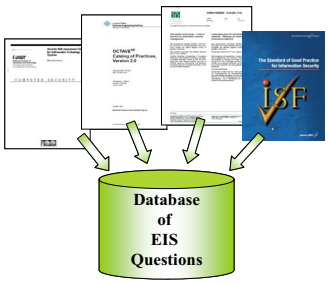

Figure 1. The area of information security is defined by several standards, which have been compiled into an EIS database of questions.

An example of a question might be: *"To what extent are intrusion detection tools installed on the systems?"* Currently, the EIS database is comprised of 1114 such questions, and together they may be viewed as defining what Enterprise Information Security is.

If we, for some specific enterprise, obtained positive answers to all the questions in the database, the company would arguable merit the highest EIS score. Inversely, if we obtained negative answers to all questions in the database, the company would arguably merit the lowest EIS score. The database of questions might then be employed to assess the level of information security on a very simple ternary scale, where companies satisfying all questions/requirements obtained the score 2, companies satisfying some questions obtained 1 and companies satisfying none obtained 0.

2.2. A Percentage Score for Enterprise Information Security

However, since most companies would end up in category 1 on the ternary scale, it would be rather useless. We have to increase the resolution of the scale.

www.manaraa.com

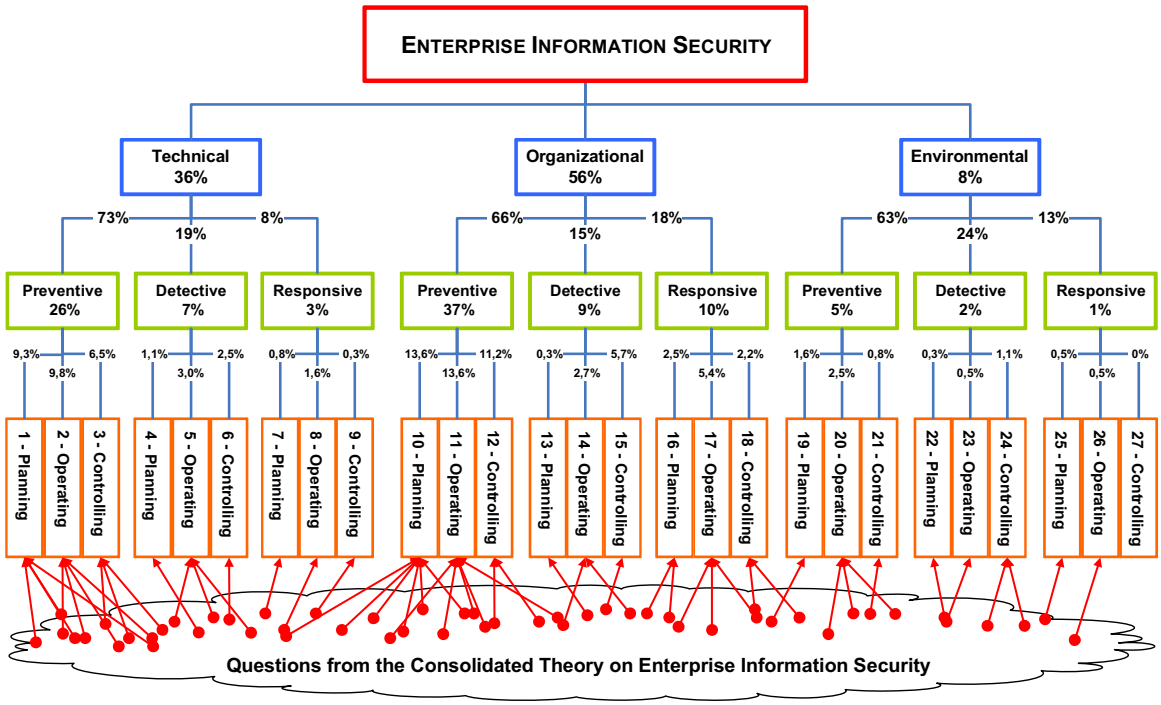

Figure 2. Illustration of the theory-based prioritized ATD on Enterprise Information Security (EIS) presented in [9] and [10]. The individual questions from the EIS database (cf. Figure 1) are located at the bottom. They are aggregated into higher-level concepts. At the top, the EIS score is represented as a weighted aggregate of all individual answers.

But, if we obtained a mix of positive and negative answers, we might not be able to determine an EIS score, because 1) the answers may not be on the same scales, and 2) different questions may be more or less important in relation to each other. In order to address the first concern, answers are mapped to a standard *scale*. To address the second issue, it is necessary to assign different *priorities* to all questions. In order to avoid prioritizing all 1114 questions in the EIS database individually we could first classify them and prioritize the classes. To present and set priorities of questions and groups of questions, the authors employ the concept of the *Architecture Theory Diagram* (ATD), further described in the work of Johnson [7] [8].

Figure 2 illustrates the ATD on Enterprise Information Security derived in previous papers [9] [10]. At the bottom of the ATD, the individual questions from the EIS database are located. These are aggregated into higher-level concepts. At the top, the EIS score is represented as a weighted aggregate of all individual EIS questions.

There are several ways in which priorities can be assigned to the ATD, for example: to view all standards as equally important; to consider the weight in relation to the number of citations; to investigate their actual use; or to let security experts, or the enterprise IT organization do the prioritization. These approaches are further explored in [10].

2.3. The imperfect answer

The most simplistic approach to obtaining a percentage EIS score would be to simply ask all questions and aggregate the answers according to the ATD. There is, however, a complication with this approach, namely the cost associated with obtaining a credible answer to an individual question [2]. In principle the more effort we spend on corroborating the answer by alternative sources etc., the more credible it becomes [14] [17]. In a previous paper a set of heuristics for assessing the credibility of answers are presented [11]. They are briefly summarized in Table 1.

Furthermore, it is conceivably resource demanding to obtain even low-credibility answers for 1114 questions. By settling for less than all answers, credibility of the EIS score is compromised. Thus, the relation between credibility and number of questions is also is increasingly dependent, cf. Figure 3.

www.manaraa.com

Table 1. Heuristics for credibility assessment

Heuristics	
Time proximity	The shorter the time since the source had contact with her source, the higher the credibility.
Hearsay proximity	The more sources between the current and the truth, the lower the credibility.
Source Persistence	The longer the answer was undocumented, the lower the credibility.
Source of Source	The lower the credibility of the source of the source, the lower the credibility of the source.
Track Record	The higher the historical credibility of the source, the higher the estimated credibility
Presentation	The sloppier the answer, the lower the credibility.
Reflected Credibility	The lower the self-assessed credibility of the source, the lower the credibility.
Referred Credibility	The more references to the source, the higher the credibility.
Expertise	The better the match is between the domain of the question and the expertise of the source, the higher the credibility.
Motivation	The closer the answer is to the politically beneficial answer for the source, the lower the credibility.
Corroboration	The more sources that give the same answer, the higher the credibility.

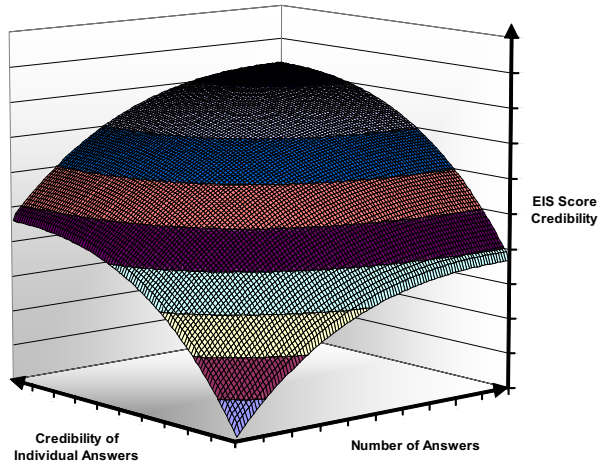

Figure 3. The total credibility of the EIS score, i.e. weighted aggregate of all individual answers in Figure 2, is dependent on the total number of questions answered as well as the credibility of individual answers.

2.4. A simple approach

The perhaps second-most simplistic approach to the problem of imperfect answers – the most simplistic approach being to answer all questions with total credibility – would be to 1) select a limited set of questions randomly and 2) use a fixed search cost for each answer. The overall credibility of the EIS score would then be dependent on the credibility of individual answers as well as total number of answered questions; this was presented graphically in Figure 3. In order to increase the credibility in this approach it would be necessary to increase the effort of answering questions

2.5. An elaborate approach

In contrast to the simple approach presented above, we here propose a more elaborate one where the credibility is improved *without* increasing the effort of answering questions. In order to accomplish this, three criteria are employed.

Choose important questions in favor of unimportant ones. Due to, for instance, varying threats and risks, different organizations prioritize differently between the 1114 questions in the EIS database. By favoring highly prioritized questions, we can improve credibility at a given effort level, cf. Figure 4.

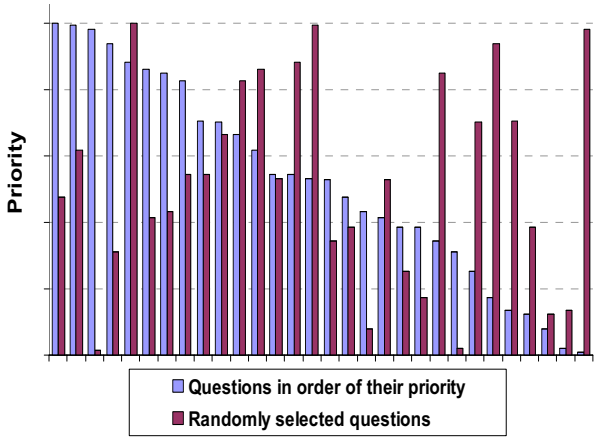

Figure 4. By answering questions in order of their priority (instead of randomly), credibility of the assessment can be improved for the same amount of effort [10].

Choose cheap questions in favor of costly ones. By favoring easy-to-find questions, we can improve the credibility of the EIS score at a given effort level, cf. Figure 5. Minimizing the effort by choosing the cheap questions is the topic of the remainder of this paper.

www.manaraa.com

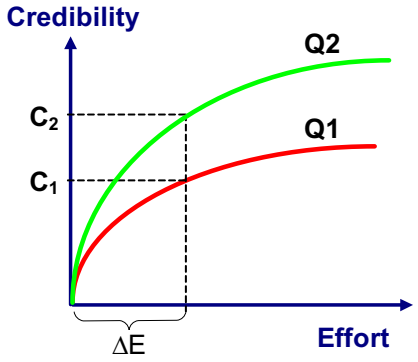

Figure 5. When answering questions it is preferable to choose the one associated with the Q2 curve than the one associated with the Q1 curve. Since the question with a favorable credibility-versus-effort curve improves credibility of the EIS score most for a given effort ΔE.

Trade-off individual credibility for statistical credibility. By optimizing the effort spent on 1) improving quality of individual answers and 2) answering more questions, we can improve credibility at a given effort level, cf. Figure 3 and Figure 6. This will be covered by a forthcoming paper.

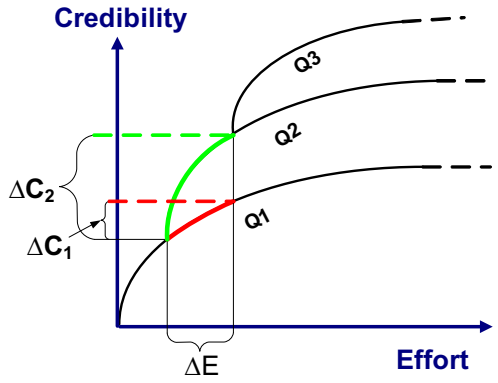

Figure 6. Maximizing the total credibility is a trade-off between the effort spent on a specific question vs. the effort spend on answering several questions.

The Complete Method. The different aspects of the EIS assessment method presented in this brief review are offered in greater detail in a series of published papers, see [9], [10], and [11]. The present paper focuses on the concept of *information search cost* predictions for Enterprise Information Security.

3. Justification for Information Search Cost Prediction Methods

As discussed previously, doing an EIS assessment is difficult and complex, not only because it of unclear definitions, but also due to the difficulty to obtain credible answers to specific questions. The reason for the latter problem is mainly that our time and resources for performing the assessment is limited; we are not willing to perform the assessment at an unlimited cost. Few, if any, methods take this into explicit account. The cost of performing assessments is generally associated with the fact that the information needed for the assessment can be very difficult to find in (or perhaps outside of) the organization. For instance, one of the questions of the EIS database is *"Are final risk determinations and related management approvals documented and maintained on file?"* Where exactly is this piece of information located? Unless you yourself know where to look or know who to ask where to look, the search can take quite a while. Moreover, an average large-size company possesses a couple of hundred IT systems, which makes questions such as *"Is the sensitivity of the system determined?"* not just a single question, but hundreds. Yet another problem is questions such as *"Are in-place controls operating as intended?"* Then, in addition to find out exactly how the controls are operating, the intention of the company has to be identified.

On the other hand, not all questions are very costly; *"Is an up-to-date copy of the contingency/disaster recovery plan stored securely off-site?"* is for instance probably not so difficult to find an answer to. So, if the information search cost issue is not adequately managed, there is a significant risk that assessment attempts fail (or at least give non-credible results.) For instance, if questions from the EIS database are picked just randomly, or prioritized according to importance, we might end up with more time consuming questions than we can afford to answer. However, if we knew in advance how difficult each individual answer would be to obtain, then we would be able to select the assessment questions in such order so that the effort is minimized. Prediction of information search cost is the topic of the next chapter.

4. Methods for Information Search Cost Prediction

In order to obtain an effective EIS assessment method we thus need to acquire estimates over how costly different questions are to answer before the actual

www.manaraa.com

assessment begins. In this paper we present two different methods to estimate the information search cost. The first method is based on experiences from the community of experts working hands-on with security analyses at enterprises. The second method provides an organization-specific indication obtained from previous EIS assessments at a certain company. These methods will be described respectively in the next two subsections.

The overall intention with developing such a method is twofold: Firstly, it serves the purpose of estimating the "price" for an EIS assessment. This will provide management with good decision support so that cost and utility of the assessment can be traded off. Secondly, and probably more importantly, the method can help identifying the answers that actually are the cheapest ones to collect so that unnecessary effort does not need to be spent on obtaining the total EIS assessment score. In this paper we make no distinction between cost and time; cost is simply measured in time.

4.1. An Organization-Independent Method

Description. This first method takes a generalist approach to identifying the cost of obtaining security information. It bases its estimation on a survey performed among experienced security assessment consultants. The expert consultants are identified as the persons with the highest trustworthiness on this subject since they are the ones that most frequently do security assessments in a real-life setting. Furthermore, in order to stay in business on a competitive market, these experts need to use their experience how difficult it is to find different types of information when calculating the overall cost for tendering assessments in the field. In the study twenty carefully selected respondents from the Swedish industry participated.

The respondents prioritized the relative difficulty of finding information within the EIS subcategories presented in section 2.2, see Figure 2. The survey was not conducted asking for some specific organization or type of organization, wherefore the results of this method can be seen as an average estimation of finding different security information in companies. In total 100 questions were picked from the EIS database (i.e. out of the base of the 1114 questions), randomly selected from the twenty most important EIS subcategories. (The prioritization of EIS subcategory importance is further described in [10].)

The respondents were asked to perform pair-wise prioritization with respect to which of two questions that is more time consuming to find the answer to. This prioritization was made with a web-based prioritization tool, FocalPoint [4], which base its analysis on the *Analytical Hierarchy Process* (AHP) [14]. This allows us to efficiently achieve statistically ensured results without having to perform prioritizations for all the possible combinations among the selected EIS questions [12]. The prioritization is made on a nine grade scale ranging from a strong opinion in favor for the first question, to neutral opinion, to a strong opinion in favor of the second question. Figure 6 shows an example of a screen dump from the prioritization tool.

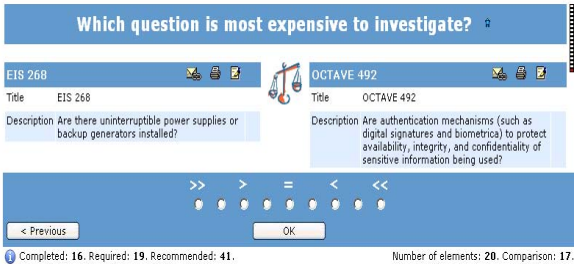

Figure 6. An illustration of a pair-wise prioritization of EIS questions using the *Analytical Hierarchy Process* [14] in the tool from FocalPoint [4].

The respondents were explicitly told to prioritize the questions with respect to finding answers with high credibility. In addition they were asked to consider only active time needed for searching the answer.

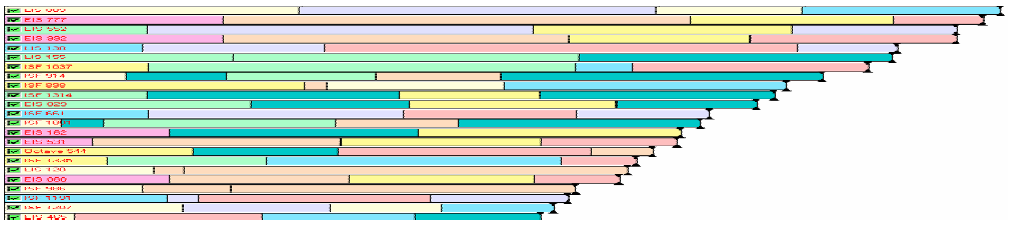

Figure 7. Illustrating a part of the ranking of EIS questions (the respondents' priorities are piled on to of each other per question).

www.manaraa.com

Results. The result of the survey was thus a range of questions ordered according to their relative estimated search cost, illustrated in Figure 7. The questions were then aggregated into their respective groups of the ATD on EIS presented in section 2.2 and Figure 2. The final aggregated prioritization is normalized on a scale ranging from 0 to 100. This scale is labeled the discoverability index, which is the inverse of the search cost.

In Figure 8, the most "expensive" category (low discoverability index) is presented to the right, and the "cheapest" category (high discoverability index) is ordered to the left.

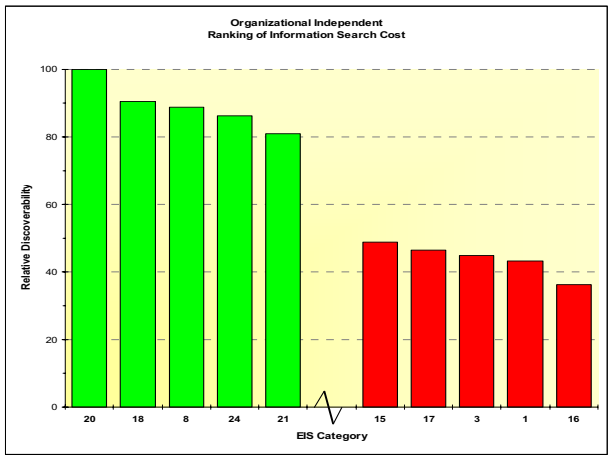

Figure 8. Estimated information search cost (presented as discoverability) for EIS categories.

4.2. An Organization-Dependent Method

A weakness with the above method is of course that we might suspect that the information search cost may vary a lot with the organization being assessed. It might consequently be relevant for a specific company to try to find a more accurate local estimate of the search cost.

Description. This method resembles of the previous but is instead based on empirical data from an actual EIS assessment performed within a large North European power company. During the investigation the assessor carefully documented the time spent on finding answers to all the questions asked. Just as in the previous assessment method, questions from the EIS database were randomly selected, even though only 60 questions this time. This reduction of the quantity of questions was due to the time of performing the assessment. For the ranking of the questions, only those that had been answered with a high credibility have been used. (This consequently is the same condition as for the previous method.) In total 48 of the 60 answers were highly credible answers.

Primarily the answers to the questions were collected by structured interviews, but also document reviews and observations were used. The credibility of all the collected answers were estimated by means of the credibility heuristics presented in a previous paper [11] summarized in Table 1, see section 2.3 above.

Results. Just as in the previous method, all the questions were grouped into their respective theoretical EIS category in the architectural theory diagram (ATD), cf. section 2.2 and Figure 2. The summarized average search cost per EIS category is presented in Figure 9. (The deviations are the result of a small sample size: in total 48 questions scattered on 20 categories).

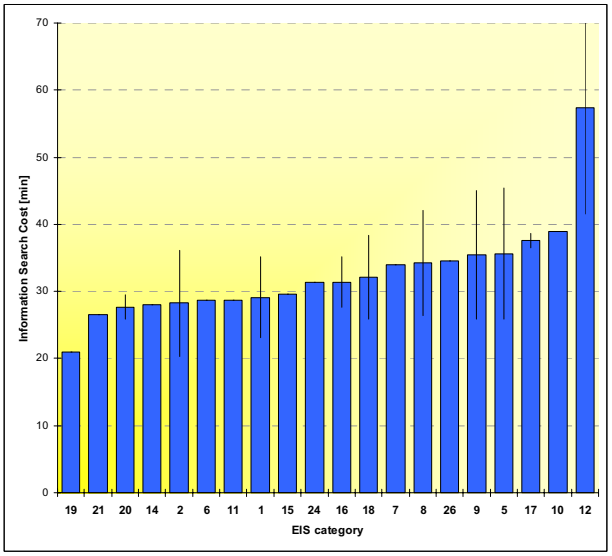

Figure 9. Information Search Cost for EIS categories (cf. figure on ATD).

5. An Efficient Enterprise Information Security Assessment Method

Recollect that the prime purpose for developing information search cost prediction methods is to be able to allow efficient Enterprise Information Security assessments. In this section we will examine how much search time that can be saved by doing an efficient selection of assessment questions. In this analysis we will use the predictions from the organization independent search cost method and estimate how much more efficient the case study could have been performed. This

www.manaraa.com

analysis will be made by comparing the different EIS assessment approaches presented in sections 2.4 and 2.5. Firstly questions will be selected randomly, secondly they will be selected according to discoverability, and finally also with respect to their importance.

5.1. Choosing questions randomly

As base for comparison, we will calculate the cost of employing a simple EIS assessment approach that is selecting questions randomly. We require a level of credibility of the EIS score allowing a deviation of 4 percentage units. (This value will be held constant in the below comparisons.) In total 28 questions had to be selected in order to achieve the required credibility level. This corresponds to a relative search cost effort of 16 hours, cf. Figure 10.

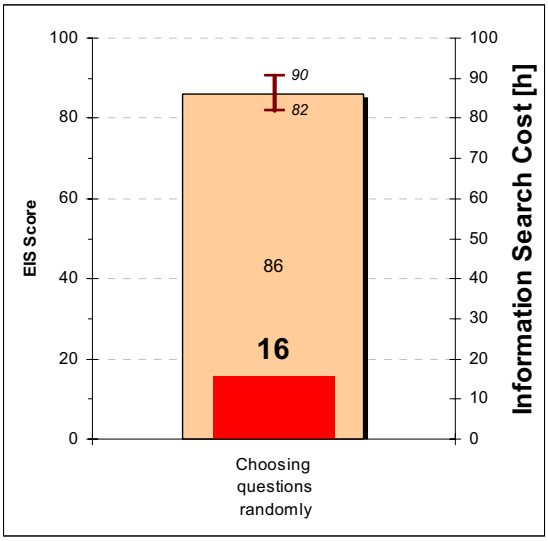

Figure 10. Total search cost for randomly chosen questions, illustrated together with the total EIS score at the studied energy company.

5.2. Choosing cheap questions

By instead selecting the cheapest questions according to the organization independent prediction method first (cf. Figure 9), we will get the indication of the EIS by only asking 24 questions, or a search cost of 13 hours, see Figure 11. (Still with the credibility level is set to a deviation of 4). The effort is thus decreased by 20% compared with the effort that would (in average) been required if we picked questions randomly.

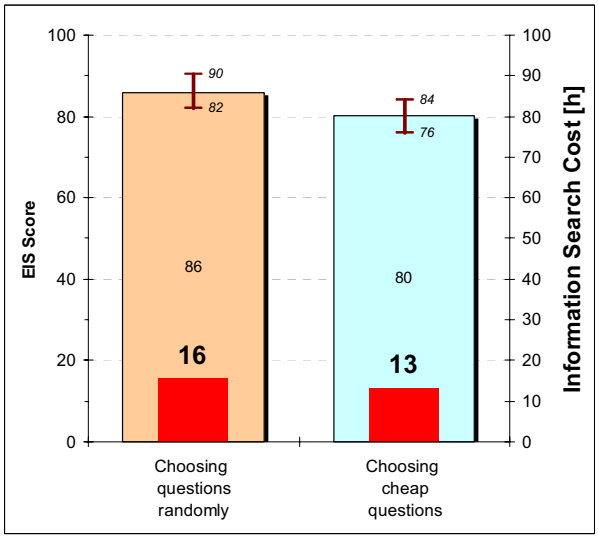

Figure 11. Illustration of the total search cost (and EIS score) when cheap questions are chosen in comparison with randomly selected assessment questions.

5.3. Choosing cheap and important questions

By selecting only the cheapest questions we have cut down the total search cost a great deal. If we follow the approach presented in section 2.5, the total search cost can be reduced even more (for the same level of credibility).

One possible prioritization of the questions is obtained by letting practical experience from key stakeholders drive the ranking of the EIS categories. If the vast majority of the stakeholders consider a particular requirement as strongly important, that should be taken into account.

In a previous paper [10] all the EIS subcategories were prioritized with respect to their importance by an expert panel from the *Swedish Information Processing Society* [16]. The prioritization were performed by 24 respondents who participated in a workshop where an AHP-based prioritization was carried out. The participants were experienced consultants/auditors working in the field of Information Security. The computer-based tool from Focal Point was applied [4].

The expert's prioritization of the EIS categories is presented in Figure 12. The result present that experts promote the "*Preventive*" measures, and that it is important to fulfill requirements of the "*Planning*"-phase. The focus of these early phases is generally found to be the efficient way to protect against vulnerabilities.

www.manaraa.com

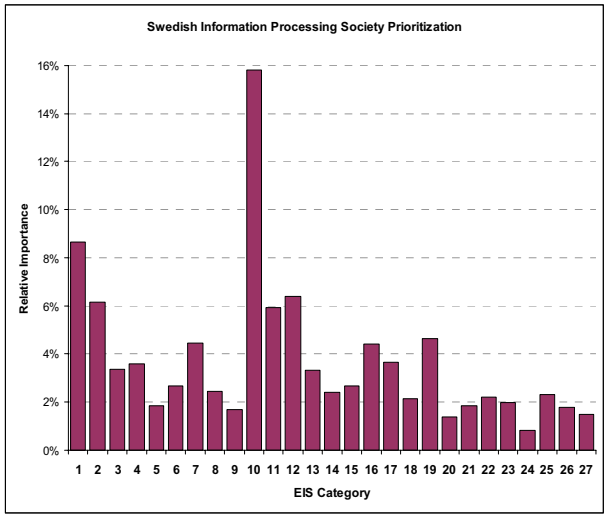

Figure 12. The prioritization of the EIS categories according to an expert panel within the Swedish Information Processing Society.

If we compare the search cost predicted by the organization independent method with the importance prioritization made by the expert panel, the relation presented in Figure 13 is found.

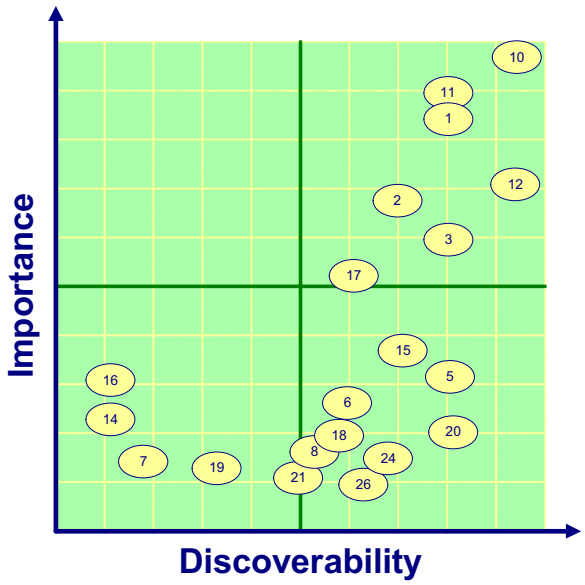

Figure 13. The *importance* of the EIS categories versus the *discoverability* predicted by the organization independent method.

With this knowledge we can trade off search cost with importance. By starting with questions in the EIS categories from the upper right quadrant (i.e. those categories that are most important and have the lowest predicted search cost) we reach our predefined credibility level by only asking 22 questions, which corresponds to a search cost of 12 hours. This gives us a third and optimized value, presented in Figure 14.

Prioritizing the questions not only after their predicted effort but also according to their importance, the total calculated efficiency gain is increased to 25%.

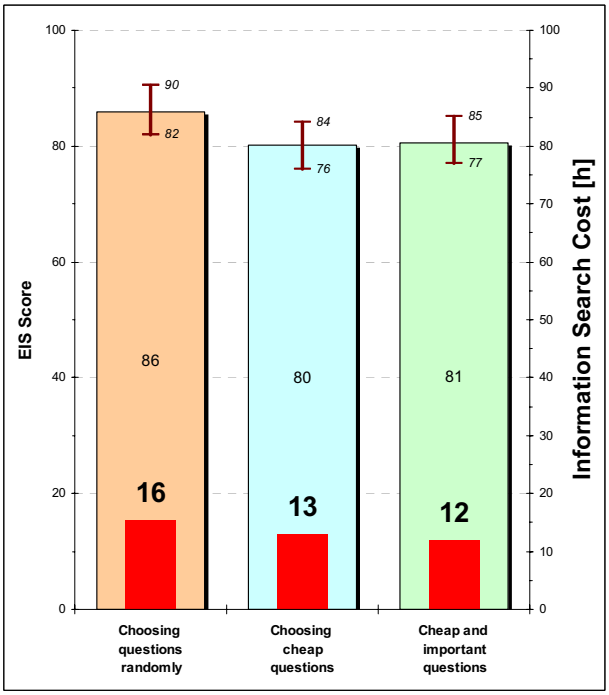

Figure 14. Total search-cost (and EIS score), the third bar illustrates the assessment result when questions are selected with respect to both importance and search cost.

6. Conclusions and Discussion

In this paper we have introduced the aspect of cost of conducting Enterprise Information Security assessments. An important factor routinely neglected is the time it takes to find all the pieces of information needed to perform assessments; we call it the information search cost, or inversely, the information discoverability. By choosing questions that are easy to find answers to, instead of do the selection randomly as is the traditional approach, we calculate an efficiency increase of 20% in an assessment performed at a large European energy company. Prioritizing the questions not only after their predicted effort but also to their importance, the total calculated efficiency gain is increased to 25%.

www.manaraa.com

Information search cost does not only pinpoint the price for acquiring information needed for well-informed decision making, it also indicates how the information base can be reorganized in order to support assessments. Identifying expensive information might help find weak spots in the organization structure; exactly why is it so difficult to find certain pieces of information? Especially this becomes essential if the most important security information also is the most difficult to get a hold of. Performing frequently re-occurring assessments in such organizations becomes very expensive. In an efficient and security-aware organization, important information should simply be easy to find, otherwise this circumstance might become a security risk in it self!

Acknowledgements

The authors would like to thank Jonas Brag and Mikael Grynblat who have contributed to this paper by conducting the major part of the data collection in the surveys. Our deep gratitude goes to the sponsor of this research, namely the global CIO Group at Vattenfall and we would especially like to mention Georg Karlén, without this work would not have been feasible.

References

[1] Alberts, C.J., et al. (2001), *OCTAVE^{SM} Catalog of Practices*, Version 2.0, Technical Report CMU/SEI-2001-TR-020 Carnegie Mellon University Software Engineering Institute, October 2001.

[2] Edvardsson B., "The Need for Critical Thinking in Evaluation of Information", *Proceedings of the 18th International Conference on Critical Thinking, Rohnert Park,* USA, 1998.

[3] Ekstedt M., et al., "Consistent Enterprise Software System Architecture for the CIO – A utility-Cost Approach", *Proceedings of the 37th annual Hawaii International Conference on System Sciences (HICSS)*, 2004.

[4] FocalPoint AB, Linköping, Sweden, viewed 10 February 2005, http://www.focalpoint.se.

[5] Information Security Forum (ISF), *The Standard of Good Practice for Information Security,* 2003, http://www.isfsecuritystandard.com; accessed May 2004.

[6] ISO/IEC International Standard 17799:2000 *Information technology - Security techniques - Code of practice for information security management*, 2000.

[7] Johnson P., *Enterprise Software System Integration – An Architectural Perspective*, Ph.D. Thesis, Royal Institute of Technology (KTH), Stockholm, 2002.

[8] Johnson P., et al., "Using Enterprise Architecture for CIO Decision-Making: On the importance of theory", *In the Proceedings of the 2nd Annual Conference on Systems Engineering Research (CSER)*, April 15-16, 2004.

[9] Johansson E., et al., "Assessment of EIS - An ATD Definition", *in the Proceedings of the 3rd Annual Conference on Systems Engineering Research (CSER)*, March 23-25, 2005.

[10] Johansson E., et al., "Assessment of Enterprise Information Security – The Importance of Prioritization", *In the Proceedings of the 9th IEEE International Annual Enterprise Distributed Object Computing Conference (EDOC)*, Enschede, The Netherlands, September 19-23, 2005.

[11] Johansson E., et al., "Assessment of Enterprise Information Security – Estimating the Credibility of the Results", *Proceeding of the Symposium on Requirements Engineering for Information Security (SREIS) in the 13th International IEEE Requirements Engineering Conference*, Paris, France, 2005.

[12] Karlsson J., et al. "An evaluation of methods for prioritizing software requirements", *Information and Software Technology 39,* pp. 939–947, 1998.

[13] Swanson M. et al (2001), *Security Self-Assessment Guide for Information Technology systems*, National Institute of Standards and Technology Special Publication 800-26, US Government printing office, Washington D.C., 2001.

[14] Pfleeger S.L., "Soup or Art? The Role of Evidential Force in Empirical Software Engineering", *IEEE Software Volume 22, Issue 1*, pp. 66 – 73, Jan-Feb 2005.

[15] Saaty T.L., *The Analytic Hierarchy Process*, McGraw-Hill, Inc., 1980.

[16] Swedish Information Processing Society (Dataföreningen i Sverige, DFS), Stockholm, Sweden, website http://www.dfs.se.

[17] Yin, R.K., *Case Study Research: Design and Methods, 2nd ed.*, Sage Publications, 1996.

www.manaraa.com