The Value and Assessment of Information Security Education and Training

Louise Yngström and Fredrik Björck
Department of Computer and Systems Sciences, Stockholm University & Royal Institute of Technology, Electrum 230, SE-164 40 Kista, Sweden. E-mail: {louise,bjorck}@dsv.su.se

Key words: Information Security Education, Information Security Awareness, and Measuring.

Abstract: Information security education and training needs to be valued and assessed from various perspectives. This study presents two differing viewpoints from which such an evaluation can be perceived – those of the individual and the organisation. Some sorts of profits are sought after by each of the two, although this is expressed and hence valued differently depending on the perspective taken. We examine the need for measuring the effect information security education and training, in addition to identifying possible techniques and problems connected with doing this in practice.

1. INTRODUCTION

The Internet evangelium is rapidly embraced everywhere – log onto "The Net" and meet new friends, order that vegetarian pizza, place a phone-call, visit the Museum of Ancient Art, groove to the latest hit, watch the news, make business the modern way - go global! Undeniably, the potential benefits are immense. However, most of us forgot that all coins usually have two sides: "You can pay me now or you can pay me later", as William Murry [1] phrases it.

In the haste to get on-line, organisations and individuals alike have sometimes ignored information security risks. Hence, today the need for information security education and training is more evident than ever.

The times when only a few experts needed education and training in information security are gone forever. Today, journalists, politicians, managers, parents, pupils, teachers and other individuals require this type of knowledge.

The times when the whole body of IT knowledge could fit into the finite domain of computer science are gone forever. Today, ethical, social, legal and economic implications of IT use must be considered - so also within the realm of information security.

The times when information security could be taught solely in a linear fashion focusing mainly on aspects of confidentiality are gone forever. Today, the information security agenda has changed - aspects such as trustworthiness of information are seen as more important. Further, the new broadened curriculum demand new pedagogical tools – ideally generalistic, interdisciplinary or holistic approaches.

As the conditions for information security education and training changes, the need for thorough evaluations and assessments are on the rise. This study presents the need for information security education and training, the need for assessing (or measuring the effects of) such efforts, and some examples of methods and problems pertaining to assessment. These three aspects tend to look very different from the viewpoint of the organisation compared to that of the individual. This paper tries to capture these differences by presenting one section about information security education and training from the point of view of the individual and one section from the viewpoint of the organisation. The idea is to show how assessment can be, and in many cases is, approached.

2. THE INDIVIDUAL'S PERSPECTIVE

2.1 The value of and need for information security education and training

It is hardly possible to develop adequately secure IT systems and information management procedures unless high quality education and training in information security is available to individuals – system developers as well as users and others.

The vast majority of all information security education and training efforts have been aimed at computer specialists, while other groups such as professional users from other disciplines as well as regular and casual users

and usees[1] have been overlooked[2]. As a result, these computer specialists have provided the world with advanced information security models, methods architectures and tools. Unfortunately, many of these have proved to be insufficient or too complex to use. Consequently, the need to educate and train also other groups of individuals in the art of information security has recently been noticed. Selected arguments from these information security scholars reiterates and reinforces this belief:

- Highland [2] suggests that the failure to develop meaningful computer security practices have to be shared by three communities: The academic community which has been lax in acceptance of computer security, the business community which was unable to specify its needs, and the military establishments which has designed models unsuitable for the real world.
- Cohen [3] suggests historical reasons; the important constituents of the information protection domain were separated into the sub-fields of cryptography, computer security, fault tolerant computing and software safety. Computer security covers leakage, fault tolerant computing covers accidental events, and special purpose systems cover selectively otherwise uncovered areas. Specifically, taken together these sub-fields do not cover the full range of information protection and security (e.g. disruption of services not attended to).
- Parker [4] argues that defining the elements of information security, as the preservation of confidentiality, integrity and availability is a dangerously oversimplified definition that has to be extended. This definition is not sufficiently comprehensive to protect information appropriately in all of its security aspects.
- Fåk [5] argues we are lacking awareness; we have a market with too many customers knowing neither what they want nor what they can get. There is no lack of basic tools but a severe lack of good implementations. Moreover, experts and practitioners are not interested in each other's questions, thus they do not communicate.

These statements should be taken seriously - lack of meaningful computer security practices, separation of the information protection domain into sub-

[1] The concept "usees" originated from within IFIP Technical Committee 9 and signifies indirect users of information technology, such as a person who relies on the computing power of some organisation he or she is a customer at without directly interacting with the technology itself.

[2] One can only speculate about the reasons, but one explanation might be that security experts did not foresee the future importance of the area, and in particular how vulnerable the whole structure may become when "everyone can do everything" without accepted rules or regulations.

areas, incomplete definitions, and inadequate awareness. They have in common that they mark the need for information security education and training, not only for computer specialists, but also for individuals in other positions. Moreover, these sceptical statements about information security imply that evaluations of today's education programmes and training efforts might be deficient.

2.2 The need for measuring

From the perspective of the individual/learner, there are several reasons why assessment of education and training efforts ought to be undertaken. This section describes some of those motives.

Existing education and training on various levels do not yet cover the full range of needs, even though there is a positive trend in numbers of courses, offered by universities and other organisations. Through making explicit areas for improvement, an assessment effort may play a significant role in ensuring that future courses and academic programmes advance to be more all encompassing.

Depending on the their present stage in life, individuals might strive to get a job, to obtain a better position, to gain higher self esteem, or to perform tasks at work more efficiently and effectively. In whatever situation the individual is in s/he is looking for knowledge that can make their life (or others) a little bit better – individuals want their knowledge to help them earn profits - not necessarily purely financial. Assessment of courses and programmes in information security can assure this in two ways: Firstly, assessment support advancing and sustaining the quality of the knowledge that is delivered to the individual[3]. Secondly, given that the assessment leads to a high quality course or programme, it will attract individuals eager to learn information security, which will further increase the quality.

The necessity to evaluate information security education and training is now apparent, although choosing the scope and the method of evaluation is not always as simple.

Wilson *et al*. [6] suggests an assessment should cover the learner's subjective satisfaction, the learning effectiveness, the teaching effectiveness and the program effectiveness. For each of these four levels there are three types of programmes - basics/literacy, training and education. This scheme covers aspects concerning the individual, the organisation and, to some extent, aspects pertaining to society. However, in the next section, we will mainly present evaluations targeting the aspects of the individual and the pedagogical methodology. Even though the outcome of such an assessment

[3] Providing that the course or programme was assessed *before* the individual participated in it.

depends on the students and teachers, organisations and societies later estimate the value of the education or training effort, e.g. on the job market.

2.3 Techniques for measuring – an example

A similar approach as mentioned by NIST [6] was applied for evaluation by Yngström [7-11] on an interdisciplinary and holistic oriented academic education in IT security. The evaluation also included assessment of a specific pedagogical methodology chosen to fit the interdisciplinary and holistic approach. The educational programmes involved were initially two one year programmes, one on undergraduate level (Bachelor) and one on graduate level (Master) at the Department of Computer and Systems Sciences, in what became labelled as the Security Informatics Programmes. These programmes were later split into smaller units, which also were involved in the evaluations. Also an evaluation of a single IT security course including the methodology, offered in a non-European university environment was included.

The development of programmes and their courses began out of need and curiosity. The Swedish Vulnerability Board had recommended all educational institutions, including universities, to initiate courses in (then) EDP security, and practical circumstances made us hypotheses that a specific pedagogical methodology using system theories[4] would be a useful vehicle to understand interactions between technical and non-technical components needed for secure IT environments. The courses were originally developed in interaction between members of the Vulnerability Board, industry and academia [12].

As an educator it is fundamental to see what happens. But how should such courses be evaluated, their main goal being to lessen vulnerability in trade, industry, government, and societies? It was quite clear from the beginning that the primary groups to be educated would be managers responsible for the enforcement and measures of safety and security in computer systems at different levels of society and organisations. Therefore the initial target group for education was specified as managers, or managers-to-be, of security in organisations which use computers, and the intent was to increase the professionalism within these groups by providing them with a specialised undergraduate degree which would also qualify for entering graduate studies[5]. The goals of the first programme on undergraduate level were stated as:

[4] The pedagogical methodology is called the Systemic Holistic Approach, which includes a specific course called the Systemic Module.

[5] Very few Swedish security managers at that time had a university degree, but a trend was starting with traditional and IT security professionals to pursuit academic studies in law,

> Of such an extension and be placed at such a level that width and depth, theoretically as well as practically, will bring the student ability to participate independently in the processes of planning, designing, implementing, evaluating systems and -functions which will lead to that the demands of reality for system survival can be realised. In this context the concept system does not only imply technical ones (like computer-, communications-) or administrative ones (information-, surveillance-) but the total reality including the artefacts needed to create stable and robust structures on different levels of society. [12] p 297.

The first evaluations were regular pedagogical ones, concerning aims and scopes, course structures, contents, levels, modes of presentation, literature, examinations, overall structure, acquired attitudes, conducts and abilities and involvement from industry. These were conducted annually from the beginning and used mainly to trim the programme. In these evaluations it also became interesting vis-à-vis the chosen target group to see how active and what specific activities outside the class room participants were involved in. This made us include various statistics in the evaluations such as previous experiences from traditional security or IT security, previous academic studies in various disciplines, memberships of professional associations concerned with IT security or other relevant areas, etc.

Not until the courses and the programme had been found good enough, i.e. the students were happy with most of the aspects and could use the knowledge at work, was it time to investigate whether the original methodological idea of using system theories was of any use to them. This was in 1991 formulated into ten practical statements and presented to all students ever in the programme five years after its start in 1986. The statements dealt with different aspects of the practical use of system theories: their contribution to the students' awareness of appropriate problems and their ability to deal with these, their contribution to students' abilities to work efficiently and effectively and their contribution to the ability of continuous learning. The statements were classified into three categories, and answers were marked on a scale 1-5; 1 being totally positive and 5 being totally negative. It was also possible to answer 'question not relevant to me'[6].

---

business administration, economics and computer science.

[6] The statements were: *Category 1*: Systems theory and related General Systems Theory, General Living Systems theory and Cybernetics, - in the following called GST etc.-, has positively contributed to my awareness of appropriate problems within the security and IT security area by facilitating my ability to: delimit problems and work tasks; specify the results of my work tasks; specify the result of my colleagues' work tasks; specify the result of a consultant's work tasks; and specify criteria for security products. *Category 2*: GST etc. has positively contributed to my ability to work efficiently and effectively by facilitating my ability to: Work with new security, or IT security, relevant products; master

In order to know something about the market's opinion of these former students' abilities and knowledge in the area, questionnaires also asked for signs of promotions and positions before and after the programme. By this time, about one third of the former students were professionals in traditional security and IT security; a group which promotions and activities it was possible to keep track of even manually. In parallel was kept also statistics of students' backgrounds, memberships, etc. This group of former students formed the Swedish Association for Information Security to promote further academic education in the area. A top priority was to increase the amount of courses, and this became the embryo to the Master programme in Security Informatics, which separate courses initially were given within the PhD programme of the Department. The evaluation of the, for the first time ran, Master programme in 1993/94 show similarities with the very first evaluations of the Bachelor programme in 1986/87; to find out whether the programme met the needs of the students and the market, and to trim it into a scientifically and pedagogically esteemed programme.

The demands for knowledge in the area changed and widened during the time the two programmes have existed; regular bachelor and master students in Computer and Systems Sciences demanded to take some Security Informatics courses during their last academic year. This made the Department divide the Security Informatics programme into four units, of which three are units of two courses each which may be chosen by regular students. This change became evident in the evaluations of 1992-94, where the usefulness of the pedagogical approach was investigated in the same way as in 1991, but this time directly after the students had finished the first unit. Many of these students had not yet started their careers and could only react to statements concerning the approach's contribution to their general abilities to handle IT security. The general statistics were also collected for further comparisons.

Since the specific methodology as such is strongly influenced by the North European movements of participatory design and Soft Systems Methodology, we were specifically interested to know how the approach would be rated in a non-European culture. Therefore the 1992-94 evaluations include reactions to the statements also from one Australian group of honour students. This group was however fairly small.

The results from the 1991 study was summarised as follows: When it came to the assessment of whether the methodology chosen positively

---

and cope with new security relevant, factors or elements; and redefine old problems and treat them effectively and efficiently.

Category 3: GST etc. has positively contributed to my ability to continuously acquire new security and IT security relevant knowledge and skills by facilitating my ability to: 9. understand new products; and 10. understand new work methods.

contributing to this group's ability of problem awareness, work efficiency and effectiveness and continuous learning, 92% agreed with this. In agreement to at least 50 % were the 50 professionals within the security area. The approach contributed the most to a person's ability to delimit and specify her own problems and work tasks, but also to her ability to specify for others, such as colleagues. Relatively high scores were attributed to specifying criteria for security products, to work efficiency and learning about new products, methods and facts. The contributions to the ability of working with new products and controlling the work of consultants scored the lowest. However, with a mean score of 45.9 persons being positive to all the ten statements, the chosen methodology is perceived to have contributed to these people's ability to cope with traditional security and IT security.

The result of the 1992-94 studies were summarised as follows: The low frequency of practical experiences in security and IT security made it impossible for the students to answer half of the statements, and also to compare reactions to all ten of them. Still, answers not referring to work experiences show high appreciation; in all the mean positive reaction to these five is 46.8 out of 60. For statements requiring work experience the positive mean was 7.6 out of 11. Based on the means, 78% were positive to the non working related statements and 69% to the working related ones.

A comparison between answers given by Australian and Swedish students was interesting but non-conclusive. Swedish answers by all - practitioners and students - were higher rated than the Australian answers and there were no particular similarities in the individual ordering of the answers between the Swedish and the Australian students. When comparing the answers between Swedish and Australian practitioners, they varied more positively in different statements[7].

A special investigation of the results of the 1991 and 1992-94 studies was made, where answers were weighted in order to be able to compare them. The findings were as follows: A simple answer would be: Yes, the approach helps in forming personal learning models and acquiring good insights; and best for Swedish university students, second best for Swedish professionals, and thirdly for Australian university students. However, we do not find it reasonable based on such small groups to predict where the approach works best. The differences in duration of presentation, possibilities to try in practise and other factors were too large, in addition to the small size of the Australian group. Judging the figures in total may at least be used as an indication, pointing to the positive reactions favour in total used pedagogical methodology. It may be reasonable to interpret the result as the Systemic-

[7] We know that the Australian course in a general course assessment performed through the QUT Students Guild was given the overall rating of the course as Great or Good in 79% of cases.

Holistic Approach and the Systemic Module facilitate individuals to assess and understand problems, increase work efficiency (doing things right) and effectiveness (doing the right things) and foster continuous learning within the field of security and IT security - provided the student has some own experience to refer to. When students do not have their own work experience, Systemic-Holistic Approach and the SM still facilitate assessment and understanding of problems, increase of effectiveness (doing the right things) and fostering of continuous learning - but in order also to increase efficiency (doing things right) practise is needed.

Assessment of the Master Programme included a question of where and if the approach had been useful. Eight of the eleven students noted "in all courses", and the other three offered varying, but positive answers. In addition all students rated the programme as a whole to have fulfilled their different educational goals positively, giving a mean of 89% of the successful students. We would regard that as qualitatively very good answers; the organisation and presentation of the content had been more than satisfying to all participants even despite different educational goals. Also the Master programme has shown to be efficient within the market for its successful participants; participants are satisfied with the programme and employers are happy to hire and promote them.

Table 1 was constructed in order to describe and discuss some other similarities and differences between the groups being evaluated in 1987, 1991, 1992-94 and 1993/94. Separate figures were taken directly out of presented material [11] or compiled based on it. Again, it is not the separate figures that are interesting, but the chart may present eventual trends and indexes.

Groups 1991 and 1993/94 are the most alike in professional attitudes and ambitions; they have a high percentage of traditional and IT security professionals with a low percentage of other professionals. At the same time the academic success rate in total of all starting students is below 50% for both groups. They also have in total the highest figures for the value of the Systemic-Holistic Approach and the Systemic Module. Other figures of interest to note are: fewer women seem to be engaged in groups with higher professional attitudes and ambitions, the age of professionals seems to be lowering, and the group is totally well educated in more than one academic discipline.

The 1992-94 group was already earlier noted as a typical university students group. It includes fewer professionals in traditional security and IT security. Members are younger, and also more women participate. The academic success rate is the highest of all groups. In total their appreciation of the SM and the S-HA is somewhat lower than the professional groups.

The 1987 group could be regard as 'old boys' - not because of its low participation of women, but because it contained an enthusiastic first lot of varied practitioners with varied backgrounds and very strong wills to build good security foundations. Their academic success rate was as high as the students group although their theoretical backgrounds initially were lower than all other groups. Members of the 1987 group later on have moved into the 1991 group. Possibly the high percentage of professionals from other areas in 1987 have become professionals in traditional and IT security in 1991. Satisfaction rates with the Systemic-Holistic Approach and the Systemic Module are for 1991: 92%, 1992-94: 69% for statements answered only by professionals and 78% for statements answered by all, and 1993/94: 89%.

Table 1. Some general characteristics of the students

	1987	1991	1992-1994	1993/1994
Population	72	155	120	26
Answers	72	71	60	11
Professionals in (IT) security	47%	70%	18%	91%
Professionals in other positions	60%	10%	38%	9%
Mean Age	33	34	30	32
Women	11%	13%	32%	9%
Academic success ratio	58/72	71/155	100/120(courses)	12/26(courses)
Theoretical Background: Computer Science	47%	70%	85%	100%
Theoretical Background: BA, Economics or Law	40%	51%	48%	100%
Satisfaction with pedagogical methodology	not asked	92%	69% pros 78% all	89%

Despite the fact that the groups as compared to each other they are quite different; 1987 being 'old boys', 1991 being IT security professionals, 1992-94 being regular university students, 1993 being a non-Swedish university group, and 1993/94 being a highly professional group, they all were in favour of the pedagogical methodology with satisfaction rates about 70-90%. It seems therefore reasonable to state that the methodology was useful to students of IT security. In addition, the strong involvement of professionals in the programmes showed that former students make good careers with increased salaries, high esteem and promotions, both as managers and specialists.

2.4 Are these results generalisable?

The presented example of evaluations is not claimed to be generalisable in detail, which was not the intentions at the time. However, the approach to evaluate the programmes on different levels as described by [NIST 1998] was followed: student satisfaction with the courses in various aspects were evaluated, the learning effectiveness and efficiency were evaluated for performances within the education as well as performances and outcomes at the workplaces, and the long run effectiveness of the programmes were evaluated career-wise for former course participants.

These evaluations and comparations were all carried out without using control groups, since at the time there were no comparable courses and programmes. Today it would be possible to use the same kind of evaluation tools: questionnaires, interviews, and inspections of examination and seminar-work results, for different courses and programmes. This would certainly, to students and educators, be of value for for instance choice of institution or course revisions and developments. However, measuring the value in some sense of information security training and education, in the opinion of these authors, needs some standard or index to be measured towards. In academic environments such standards exist, although they may vary from country to country, from university to university or from one professional group to another. In the information security area for professionals, such standards also exist in various types - typically named certificates[8], - initiated as a qualitative metric. We believe all such certificates, academic as well as professionals will be of use, but we also acknowledge that the area of information security is a moving target, hence a certificate of some kind will not suffice as a general measurement, but has to be supplemented with something; maybe some form of index which will consider at least the age and content of the separate certificates. But not only is the area of information security a moving target, it is also partly a context-oriented issue - it is global in the sense of networking possibilities and it is local in the sense of existing social values and particular application areas. Such factors should probably also be weighted into an index.

[8] For example Certified information Systems Auditor CISA from ISACA, and Certificate in Information Security Management as suggested by the ISEB of the British Computer Society.

3. THE ORGANISATION'S PERSPECTIVE

3.1 The value of and need for information security education and training

From the viewpoint of an organisation, information security not only promises to assist safeguarding information assets at a given cost but, more importantly, it can provide the organisation with a competitive advantage through lower costs[9] and new business opportunities[10] (e.g. [13, 14]). Thus, organisations – from corporations through hospitals to government agencies – are increasingly becoming aware of the need to safeguard their information. At the organisational level, this is usually accomplished utilising technical as well as procedural measures – all of which depend upon human behaviour and skills to perform, for example:

Technical measures: Installing, configuring and maintaining a secure firewall will only succeed if the persons involved understands the elementary concepts of TCP/IP network traffic, have a good grasp of what inbound and outbound communications are needed, and are familiar with the interfaces used to accomplish the tasks at hand.

Procedural measures: Handling information in the way described by an organisation's information classification scheme might require the understanding of how, for example, one uses the backup system on the office workstation and how one can positively verify the sender of a digitally signed document.

This fact – that the human factor is one of the most significant determinants of the overall success of information security efforts in an organisation has been pointed out in several recent empirical studies on information security in organisations. The following citations confirm this actuality:

- Employees' information security awareness is perceived as the most important means to overcome the security problems.[11] [15]
- According to RRV it is important that awareness of computer related crime and abuse is raised within the management structure of organisations. It should be a primary priority of management to work to

[9] For example, information security might lower costs directly through a reduction of information security breaches and indirectly through more reliable IT-support for organisational processes.

[10] For example, information security can be viewed as a "business enabler" in relation to the creation of extranets for on-line banking applications.

[11] Based on a survey concerning information security answered by 428 persons, mainly IT-managers, in Swedish organisations.

reduce the risk and threat from the different kinds of computer crimes. These problems can not simply be solved by buying-in more technology.[12] [16]

– This study's main conclusion is that the respondents consider the main threat against the organisations' EDP stored information to be employees' unintentional and erroneous change and deletion.[13] [17]

By now it is evident that most organisations seems to need information security education and training, and that they are likely to benefit from information security education and training efforts. However, organisations do not usually dedicate resources for projects with no measurable impact.

3.2 The need for measuring

Managers make organisational decisions in a way similar to the way most individuals make personal decisions – with bounded rationality. That is, they try to reach the optimal decision, from the viewpoint of the organisation's purpose, given the information available at the time of the decision. Decisions regarding investments in information security education and training are also likely to follow a similar decision process. Strategic decisions (those that have a considerable impact on the organisation) are usually approached in a more structured manner than less consequential operational or tactical decisions. Regardless of the importance of a given decision, some kind of cost-benefit analysis is always carried out before a decision is arrived at – either implicitly or explicitly. Given that organisations have a finite amount of resources[14] to employ in the pursuit of its mission, investments in information security education and training must compete against other possible investments. A simplified example illustrates how organisations generally reach decisions regarding investments:

A manufacturer of studio quality microphones has 100.000 Euro reserved for investments in a given period of time. There are many different areas in the organisation that would benefit from new investments, such as a new microphone-assembly machine. In addition, there is a need for a comprehensive information security education and training programme. However, the monetary resources will not be sufficient for all desired investments, so a choice has to be made. Given the dissimilar nature of these investments, the impact of each will first have to be translated into monetary

[12] Survey on computer crime, based on answers from 1304 organisations with over 50 employees in Sweden

[13] Based on a survey about threats to EDP-stored information answered by 162 IT-managers working in Sweden.

[14] For example monetary, information, and human resources.

terms, so that a comparison is possible. Moreover, since these investments (if realised) will have an economic impact on the organisation at different moments in the future, the value of money must be converted into a common point in time – for example the day of the decision[15]. Let us have a look at the two competing options.

3.2.1 Alternative I - investing in the machine

The new machine would cost exactly 100 K Euro and result in yearly operating costs of 10 K Euro for each of the subsequent five years. After this period, the machine would need to be replaced, but it could be sold for an estimated 5 K Euro.

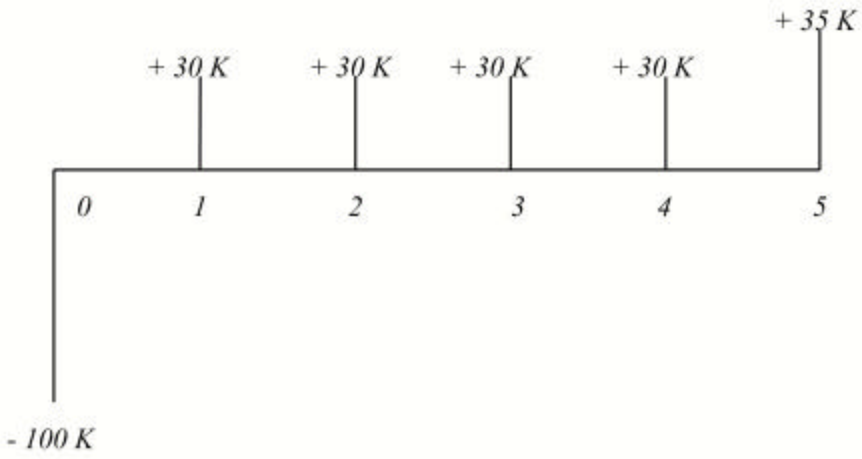

Figure 1. Expected payment flows resulting from investment in the microphone-manufacturing machine

The machine would produce microphones using the components put into the four containers on the side of it. Based on sales statistics from previous years, the microphones produced by this machine will generate 60 K Euro in sales each of the five years, of which roughly 20 K Euro are costs for components, marketing, Etc. Thus, the net payments generated by this

[15] This is because 1 Euro today is more worth then 1 Euro in ten years, since if the organisation have the coin today, they can put it into the bank (or make an investment with it) and earn interest.

investment during these five years following the initial investment will be 30 K Euro (60 K Euro for sales payments, less the 20 K Euro for components and various costs, less the 10 K Euro for the machine's operating costs). If the machine is sold as predicted, the final year of operation will result in an additional 5 K Euro of net payments. These flows of payments are illustrated in figure 1.

The value of this investment alternative can be calculated as the sum of all transactions relevant to the investment – in this case:

(-100) + (+30) + (+30) + (+30) + (+30) + (+30) + (+35) = 85 K Euro

However, since the payment flows take place at different moments in time, they need to be converted into their present value, taking into account the cost of capital[16] (interest rate). This is because the resources could have been used for some other investment which would have produced a calculated payoff or R.O.I.[17]. Let us assume that if the organisation would not have used the money for this investment, it could have bought some stocks instead and these would yield 15% R.O.I. per year. Therefore, this is the estimated capital cost if investing in the machine. Consequently, the present value *PV*, of the net payments of (for example) the third year can now be calculated as:

$$PV = \frac{C}{(1+r)^t} \quad = \quad PV = \frac{+30}{(1+0.15)^3} \quad \approx \quad 20 \text{ K Euro}$$

Where C = *capital*
r = *interest rate*
t = *time period*

Figure 2. The present value of investing in this alternative

All of the net payments (including the initial cost of the machine) resulting from this investment alternative will have to be converted into their present value if we want to be able to compare this investment with the investment in information security education and training. With this conversion, we will end up with the investments net present value *NPV*, as illistrated in figure 3.

[16] Sometimes referred to as the "alternative cost" of a given investment.
[17] R.O.I. is short for return on investment.

$$NPV = C_0 + \frac{C_1}{1+r} + \frac{C_2}{(1+r)^2} + \ldots + \frac{C_n}{(1+r)^n} \quad or \quad NPV = C_0 + \sum_{k=1}^{n} \frac{C_k}{(1+r)^k}$$

$$NPV = 100 + (30 / 1.15) + (30 / 1.32) + (30 / 1.52) + (30 / 1.75) + (35 / 2.01) \approx 103 \text{ K Euro}$$

Where *NPV = net present value*
C_0 = initial payment for the investment
C_k = other net payments
r = interest rate
n = number of payment periods (years)

Figure 3. The net present value of investing in this alternative

As we can see in the calculations above, the net present value of the investment in the microphone-manufacturing machine is 103 K Euro. This can be interpreted as "If we take into account that the alternative investment would have given us 15% interest rate, we would gain 103 K Euro if we invested in the machine". Now it is time to compare this investment with that if investing our resources in the information security education and training programme. Converting the information security education and training investment into its *NPV* makes the two investments comparable – the one with the highest NPV is the one the resources should go into if we are to make the optimal investment decision.

3.3 Alternative II - investing in information security education and training:

The ISET programme would consist of an information security awareness project aimed at different parts of the organisation, as well as some specialised information security courses for the individuals co-ordinating the information security activities in each department. The whole ISET programme would mean an initial investment (for course material, speakers, teachers, and external courses, Etc.) of 50 K Euro, and additional yearly costs of 10 K Euro for each of the subsequent five years. After these five years, the program will be evaluated. Naturally, the information security education and training investment does not have any residual value that can be converted into funds the final year, since it cannot be sold or transferred to another organisation with ease. So far, we have identified the following flow of payments for this investment alternative (Figure 4).

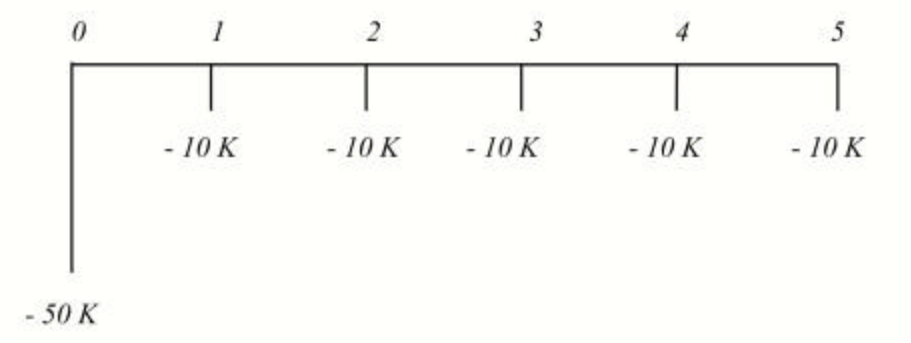

Figure 4. Expected payment flows resulting from investment in the information security education and training programme

Investment calculations usually only take into account the direct payment flows that result from the analysed investment. Therefore the investment in information security education and training does not look very good in comparison with the investment in alternative I. In fact, as observable in the calculation below, investment in the information security education and training programme will result in a negative *NPV* unless other payment flows than the calculated yearly costs can be identified:

NPV = - 50 + (-10 / 1.15) + (-10 / 1.32) + (-10 / 1.52) + (-10 / 1.75) + (-10 / 2.01) » - 83 K Euro

The investment in information security education and training is likely to have a long-term economic impact on the organisation, in terms of cost reduction due to less severe and fewer information security breaches. Also, the information security education and training programme might possibly enable new business transactions to take place, as pointed out in previous sections of this paper. If organisations are to choose the investment in an information security education and training programme instead of other investments, indirect payments flows resulting from this decision must be taken into account.

From the example, it is evident that organisations will have to try to measure the impact of information security education and training if it is to be a viable investment at all. Unless organisations are given the tools to identify the value of their education and training programme, they will not be able to justify such an investment. As a result, resources will be invested in other areas with a measurable payoff.

This section has made explicit how organisations take decisions regarding where to invest its limited resources. It has thereby clarified why organisations need to measure the impact of information security education and training. This leads us over to a discussion on possible information security education and training metrics and the problems associated with measuring.

4. METHODS AND PROBLEMS OF MEASURING

While measuring the impact of information security education and training, one is actually trying to measure the resulting change in human behaviour and its impact on the organisation's ability to reach its goal. There are several problems associated with measuring the impact if an organisational information security education and training effort, such as:

4.1 Discrepancy between what people say and what they do

The mere fact that employees, through an information security education and training programme, arrive at a measurable raised awareness of the information security regulations does not signify that they actually follow these rules or values – at least not all of them. Further, when trying to measure the impact of information security education and training, there is a possibility that some employees do not want to state the truth about their own level of awareness. They might be anxious concerning what the employer's reaction would be if they admitted that they did not know of the rules they were supposed to adhere to. Therefore, from an organisational perspective, the focus should not be on what an employee know about information security, but rather what she does with this knowledge.

4.2 Interpreting the numbers

Common sense tells us that it will be hard, or maybe even impossible, to put a number on "soft" issues, such as information security awareness (e.g. [18]). However, exact numbers are very seldom needed for an informed decision. Rather, some kind of grading, judgement or comparison is often needed. Another problem is that once numbers are produced, it might be hard to interpret them. What does it mean, for example, if the level of information security awareness is around 70%? Is this good, or is it bad? The exact answer is; we don't know. In order to interpret numbers like these, the context have to be clear – is it a bank, or is it a fast food chain? How

dependent are they on their information? Quantification of "soft" issues is more useful if it can be compared with something else as a reference. For example, the level of information security awareness as measured in one financial institution might be seen in the light of the measured average level of information security awareness in all other financial institutions in that region (given that the method for measuring was the same).

4.3 What should be measured

Information security education and training is an extensive concept in itself - it embraces many facets of information security. In our view, information security awareness is manifested in the behaviour of the humans enlightened with it. This means that the action created by mindful humans causes effects measurable only outside the finite domain of human knowledge or behaviour - in the technical and procedural elements of the organisations information system. Since some, or presumably large proportions, of these effects are directly caused by the intellectual capital labelled information security awareness, one can conceive that the estimation of these must be conducted within the formal and technical domains.

Assuming that investment decisions approximately follow the decision method outlined in the example in the previous section, organisations can not be satisfied with measuring or predicting an information security education and training programmes impact on employees knowledge only. No, this raised awareness must result in a corresponding change in human behaviour. In addition, this change must result in either lowered costs or increased revenue.

5. CONCLUSIONS

This study has demonstrated how differing the viewpoints of the organisation and the individual are when it comes to information security education and training.

Individuals - we do not only mean computer specialists - need for information security education and training to be able to minimise their security risks that they are, and will be, exposed to today, and in the approaching information society. In addition, they want this kind of training to make them appear more valuable for the organisations. Organisations' needs are often more directly connected with their financial mission or goal. This often means that they look for information security education and training to lower costs arising from information security breaches or for enabling new business opportunities.

Organisations need to measure the effects of information security education and training because of their decision process for investments. Looking at these education and training efforts as any other investment, they demand a reasonable "return on investment". If they are not provided with methods to measure the effects of, for example, a training programme, they will not be able to identify changing cost or income structures resulting from this effort. This leads to that the investment in education and training will look less favourable than it really is.

From the viewpoint of individuals, assessment of these education and training efforts should ideally focus on the knowledge content. Organisations, although indirectly attracted by the knowledge, are often more interested in the behavioural changes a given course or programme can result in. This is, as we have seen, because the knowledge has to result in some change in behaviour if it is to be valuable not only for the individual, but also for the organisation.

Individuals are looking for profit and so are the organisations, but their respective approaches and focuses in regard to value and assessment of education and training are incompatible.

REFERENCES

[1] W. Murray, "Security Should Pay: It Should Not Cost," presented at Information Security - the Next Decade. IFIP TC11 eleventh international conference on information security, 1995.

[2] J. Highland, "Perspectives in Information Technology Security," presented at Education and Society - Information Processing '92, 1992.

[3] F. B. Cohen, "Viruses, Corruption, Denial, Diruption, and Information Assurance," presented at Information Security - the Next Decade. IFIP TC11 eleventh international conference on information security, 1995.

[4] D. B. Parker, "A New Framework for Information Security to Avoid Information Anarchy," presented at IFIP TC11 eleventh International Conference on Information Security, IFIP/Sec '95, London, 1995.

[5] V. Fåk, "Unused tools are useless or Why is the gap between theory and practice in network security so wide," presented at IFIP TC11 eleventh international conference on information security, IFIP/Sec'95, South Africa, 1995.

[6] M. Wilson, D. E. d. Zafra, S. I. Picher, J. D. Tressler, and J. B. Ippolito, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," National Institute of Standards and

technology, Gaithersburg, NIST Special Publication 800-16, April 1988 1998.

[7] L. Yngström, "Experiences from a one-year Academic Programme in Security Informatics," presented at Fifth International Conference on Computer and Security, Queensland, Australia, 1988.

[8] L. Yngström, "Experiences from a one-year Academic Programme in Security Informatics," *Information Age*, vol. 11, pp. 77-82, 1989.

[9] L. Yngström, "Security Informatics 1985-1991. An assessment," Department of Computer and Systems Sciences, Stockholm University, Stockholm SIIS-R-91, 1991.

[10] L. Yngström, "Evaluation of an academic programme in IT Security 1985-1990," presented at Computer Security: Discovering Tomorrow, Proceedings of IFIP/SEC'93, 1993.

[11] L. Yngström, "A systemic-holistic approach to academic programmes in IT security," in *Report series - Department of Computer & Systems Sciences 96:21*. Stockholm: Stockholm University, 1996, pp. 176.

[12] L. Yngström, "Education in Safety Systems and Security Analysis - Suggestions for a One Year University Program," presented at IFIP/Sec'83 First Security Conference, Stockholm, Sweden, 1983.

[13] D. B. Parker, "The Strategic Values of Information Security in Business," *Computers & Security*, vol. 16, pp. 572-582, 1997.

[14] C. C. Wood, "Using information Security to Achieve Competetive Advantage," *Computers & Security*, vol. 10, pp. 399-404, 1991.

[15] F. Björck, "Information Security Survey - Sweden 1998," Ernst & Young, Stockholm, Company Report 1998.

[16] Riksrevisionsverket, "Datorrelaterade missbruk och brott - en kartläggning gjord av effektivitetsrevisionen," Riksrevisionsverket, Stockholm 1997:33, 1997.

[17] H. Johansson and M. Kager, "Perceived Threats Against Information in ADP-Systems. A Study of Swedish DP-Managers Perception.," in *Information Management.* Stockholm: Stockholm School of Economics, 1995, pp. 54.

[18] G. S. Dhillon, "Interpreting the management of information systems security," in *The London School of Economics and Political Science*. London: University of London, 1995.