A conceptual foundation for organizational information security awareness

Mikko T. Siponen
University of Oulu, Department of Information Processing Science, Finland

Keywords
Information systems, Computer security, Data security, Education

Abstract
The current approaches in terms of information security awareness and education are descriptive (i.e. they are not accomplishment-oriented nor do they recognize the factual/normative dualism); and current research has not explored the possibilities offered by motivation/behavioural theories. The first situation, level of descriptiveness, is deemed to be questionable because it may prove eventually that end-users fail to internalize target goals and do not follow security guidelines, for example – which is inadequate. Moreover, the role of motivation in the area of information security is not considered seriously enough, even though its role has been widely recognised. To tackle such weaknesses, this paper constructs a conceptual foundation for information systems/organizational security awareness. The normative and prescriptive nature of end-user guidelines will be considered. In order to understand human behaviour, the behavioural science framework, consisting in intrinsic motivation, a theory of planned behaviour and a technology acceptance model, will be depicted and applied. Current approaches (such as the campaign) in the area of information security awareness and education will be analysed from the viewpoint of the theoretical framework, resulting in information on their strengths and weaknesses. Finally, a novel persuasion strategy aimed at increasing users' commitment to security guidelines is presented.

Information Management & Computer Security
8/1 [2000] 31–41

[ISSN 0968-5227]

1. Introduction

The term "information security awareness" is used to refer to a state where users in an organization are aware of – ideally committed[1] to – their security mission (often expressed in end-user security guidelines). Information systems (IS) can be useful only if people use them (Mathieson, 1991). Similarly, information security awareness is of crucial importance, as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness (e.g. Hoffer and Straub, 1989; Goodhue and Straub, 1989; Ceraolo, 1996; Straub, 1990; Straub and Welke, 1998). Increased awareness should minimize "user-related faults"[2], nullify them in theory, and maximise the efficiency of security techniques and procedures from the user point of view. To do this at an organization level, it is important, for example, to identify, quantify and understand the background to and underlying reasons for the "human errors" in question. This should be done systematically, by establishing a programme based on or reflecting a framework such as the following one by NIST (1995, 1998): identify programme scope, goals and objectives; identify training staff and identify target audiences; motivate management and employees; administer the programme; maintain the programme and finally evaluate the programme (different feedback and measurement activities should also be developed and implemented at each stage as a source of continuous evaluation and improvement).

Although educational or awareness issues (from simply information security guidelines to well-developed information security education programmes) are security matters in nearly all organizations in the era of the information society, their nature is not well understood resulting, for example, in ineffectiveness of security guidelines or programs in practice. In this regard it will be shown that even passing around security guidelines in a factual manner per se, for instance (i.e. their presentation as normal facts, at the phrastic level), as is likely to be the case in most organizations, may be an inapt approach as such.

To increase understanding of problems relating to awareness, two categories can be outlined, framework and content (although the first, in an abstract sense, subsumes the second). The framework category is more an area of "engineering disciplines", containing issues that can be approached in a structural manner and by quantitative research, that may be formalized and are a matter of explicit knowledge[3]. The content category, on the other hand, constitutes a more informal interdisciplinary field of study, a "non-engineering area" (i.e. uses something other than mathematics and/or philosophical logic as its main reference discipline), includes tacit knowledge as well, and should be approached using qualitative research methods. The aforementioned awareness framework put forward by NIST is as it stands an example of the framework category. Almost all measures aimed at increasing awareness have focused on the first area[4] (e.g. standards and articles – see Table I and[5]), although shortcomings in the second area usually invalidate them by taking over the entire awareness programme and all its resources (people, time, money, etc.) and by wasting security techniques (such as when users fail to follow the prescribed actions). How we really motivate employees to comply with information security guidelines, for instance, is a matter that lies within this content category.

In terms of this presentation of the nature and types of awareness (Table I), this paper concentrates on the content facet, which, in

spite of its significant role, seems to lack adequate foundations. To begin with, current approaches (e.g. McLean, 1992; NIST, 1995, 1998; Perry, 1985; Morwood, 1998), are descriptive in nature. Their inadequacy with respect to point of departure is partly recognized by McLean (1992), who points out that the approaches presented hitherto do not ensure learning. Learning can also be descriptive, however, which makes it an improper objective for security awareness. Learning and other concepts or approaches are not irrelevant in the case of security awareness, education or training, but these and other approaches need a reasoned contextual foundation as a point of departure in order to be relevant. For instance, if learning does not reflect the idea of prescriptiveness, the objective of the learning approach includes the fact that users may learn guidelines, but nevertheless fails to comply with them in the end. This state of affairs (level of descriptiveness[6]), is an inadequate objective for a security activity (the idea of prescriptiveness will be thoroughly considered in section 3).

Also with regard to the content facet, the important role of motivation (and behavioural theories) with respect to the uses of security systems has been recognised (e.g. by NIST, 1998; Parker, 1998; Baskerville, 1989; Spruit, 1998; SSE-CMM, 1998a; 1998b; Straub, 1990; Straub *et al.,* 1992; Thomson and von Solms, 1998; Warman, 1992) – but only on an abstract level (as seen in Table I, the issue is not considered from the viewpoint of any particular behavioural theory as yet). Motivation, however, is an issue where a deeper understanding may be of crucial relevance with respect to the effectiveness of approaches based on it. The role, possibilities and constraints of motivation and attitude in the effort to achieve positive results with respect to information security activities will be addressed at a conceptual level from the viewpoints of different theories.

Table I
The two categories of information security awareness and current research

Category	Current research	M/B	RM
Framework	SSE-CMM (1998a, 1998b);	No	AE
	NIST (1995, 1998);		AE
	Perry (1985);		AE
	Thomson and von Solms (1997);		CA
	Morwood (1998)		AE
Content	McLean (1992);	No	CA
	Spurling (1995);	particular	EA
	Thomson and von Solms (1998)	theory	CA

Note: For full details of M/B, RM, AE and CA, see [5]

The scope of this paper is limited to the content aspects of awareness (Table I) and further end-users, thus resulting in a research contribution that is: a conceptual foundation and a framework for IS security awareness. This is achieved by addressing the following research questions:

- What are the premises, nature and point of departure of awareness?
- What is the role of attitude, and particularly motivation: the possibilities and requirements for achieving motivation/user acceptance and commitment with respect to information security tasks?
- What approaches can be used as a framework to reach the stage of internalization and end-user commitment?

Conceptual analysis, in the terms of Järvinen (1997), is used as the main research method in this paper, while philosophy and psychology are used as reference sciences. Recalling the classification of the stages of development of an awareness/education programme put forward by NIST, the objective of this study fits the "motivate employees" part, mainly excluding other issues with respect to such a framework as being beyond the scope. Questions of how to be aware of "security awareness" and how to raise the degree of awareness at the managerial level and among third parties also go beyond the scope of this paper, which focuses on "human errors" made by ordinary end-users[7] especially at the organization level (e.g. security guidelines are not followed). The intention of this paper is not to deal with the education of information security professionals. An early version of this paper was presented in Siponen and Kajava (1998).

This paper is organized as follows. The second section outlines the behavioural framework, consisting of selected motivation/behavioural theories that will be applied throughout the rest of the paper. Section 2.2 considers how people respond to awareness activities. The current methods available to increase awareness are considered in section 2.3 from the viewpoint of the theoretical framework. In the third section, the prescriptive nature of awareness will be introduced and justified. The fourth section outlines a set of approaches reflecting the prescriptive nature of awareness (and the theoretical framework described in section 2) that can be used as a point of departure to achieve the prescriptive stage of awareness. Finally, the key points of the paper are discussed.

2. The theoretical framework and selected current methods for increasing awareness

2.1 Motivation and attitude

It is generally agreed that performance depends on ability[8], motivation and working conditions (Bartol and Martin, 1994). These factors interact constantly: the effects of motivation on performance depend on ability and vice versa (Bartol and Martin, 1994). It is traditionally seen that motivation tends to be dynamic in nature (lasting from minutes to weeks) whereas attitude is a more static, internalized factor (lasting from months to years). Attitude relates mainly to the quality of actions, while motivation correlates with activity levels. According to Fishbein and Ajzen (1975, p. 388), there are two ways of producing change in human beliefs, active participation and persuasive communication (a persuasive communication strategy that can be used together with active participation is depicted in section four). The behavioural framework (shown in Table II) will be depicted and applied further.

TPB (Ajzen, 1991), the theory of reasoned action (Fishbein and Ajzen, 1975) and TAM (Davis, 1989) have attracted the interest of many IS scholars, and have been observed to be highly valid (see Chau, 1996 on TAM and Mathieson, 1991 on TPB) and are therefore selected here. Mathieson (1991), for example, has compared TAM and TPB, while Adams *et al.* (1992), Chau (1996), Igbaria and Zinatelli (1997), Straub *et al.* (1997) have used or considered TAM. The theory of intrinsic motivation is selected as it seems to explore the role of motivation in greater depth than TPB. In addition, the idea of intrinsic motivation (i.e. the crucial role of self-determination and internal reasons) has interesting connections with philosophical doctrines (e.g. the well-known "overriding" thesis of R.M. Hare that will be considered in section 4) and the doctrine of intrinsic motivation sounds persuasive.

Table II
Selected theories and their key points

Selected theories	Key issues
A theory of reasoned action (Fishbein and Ajzen, 1975); Theory of planned behaviour TPB (Ajzen, 1991)	Intention->behaviour Intention consists of attitude, subjective norms (Fishbein and Ajzen, 1975) and perceived behavioural control (Ajzen, 1991)
Intrinsic motivation (Deci, 1975; Deci and Ryan, 1985)	Intrinsic motivation: self-determination
The Technology Acceptance Model (Davis, 1989)	System use depends on behavioural intention to use, which consists of usefulness and ease of use

A good overview of these motivational/behavioural theories can be found in Locke (1991).

The theories of Fishbein and Ajzen (1975) and Ajzen (1991) are based on the assumption that intention "is the immediate determinant of the corresponding behaviour" (Fishbein and Ajzen, 1975 p. 16). Intention is divided into I1) "attitude toward behaviour" and I2) "subjective norm concerning behaviour". Ajzen (1991) has further developed the theory of planned behaviour, in which there is a third element "Perceived behavioural control" (Ajzen, 1991 p. 182). Attitude (1) consists of beliefs concerning consequences of behaviour, and subjective norm (2) consists of (2a) normative beliefs (by others) and (2b) motivation to comply (Fishbein and Ajzen, 1975 p. 16). With regard to security guidelines, the normative beliefs may arise due to an "organizational norm/culture" or role responsibility, including compliance with security guidelines/security mission/role. With regarding to the first element (attitude), we are interested in users' beliefs concerning the consequences of living up to security guidelines. In practice, the satisfying of the attitude element (1) means that the consequences of executing security guidelines must be desirable. Several approaches for making security guidelines appear desirable in such a manner will be suggested in section 4. The third element, the concept of "Control Beliefs and Perceived Facilitation" (henceforth CBPF) contained in Ajzen's (1991) theory of planned behaviour refers to "people's perception of the ease or difficulty of performing the behaviour of interest" (Ajzen, 1991, p. 183). This is best taken care of by technical education (e.g. increases in skill/ability), which – it is hoped – will make adherence to security guidelines very easy.

According to the technology acceptance model (TAM) of Davis (1989), systems use depends on behavioural intention to use, which in turn implies attitude towards use, which is divided into two elements:

1 "perceived usefulness"; and
2 "perceived ease of use".

Achieving usefulness in terms of TAM requires in practice, somewhat similarly to TPB (Ajzen, 1991), that the consequences of executing security guidelines must be desirable in the eyes of the users. Ease of use (2) seems to be close to TPB's "perceived behavioural control", and is therefore also tackled along with education. As seen, TAM is close to TPB. This is no wonder since it is greatly influenced by the theory of reasoned action of Fishbein and Ajzen (1975).

The issue of intrinsic motivation has been discussed most notably by Deci (1975) and Deci and Ryan (1985). In the case of intrinsic motivation, people have to feel free to make their own choices concerning their behaviour (self-determination), i.e. they need to justify their actions in terms of internal reasons such as their own aspirations. In essence, self-determination is the primary deciding factor determining whether someone is intrinsically or externally motivated (Deci, 1975 and Telanne, 1997). In that light, as far as security guidelines are concerned, one may argue that users seem to be more externally motivated than intrinsically.

Although delegated security guidelines (e.g. consisting of rules such as "choose a password in system X that is more than ten characters long and does not contain words that are easily guessable") may not appear to be internal aspirations at first sight, they may not prove to be a barrier to intrinsic motivation. In the end, the crucial question is whether internal aspirations, abilities and external forces (security guidelines in this case, and also normative beliefs in terms of TPB) reflect one's feeling of freedom. Active programmes (active participation) turn out to be useful in this respect by enabling a certain degree of user interaction. They also help to meet an important challenge, namely how security people can instil such a feeling of freedom in end-users that they are keen on taking an active part in the security process[9] because they feel that they are involved in security-related decision making?[10]. Some approaches to achieving intrinsic motivation through persuasion strategy will be considered in section 4. According to Deci (1975), other elements of intrinsic motivation include excitement and a feeling of being challenged. Other researchers also include the feeling of being respected (Telanne, 1997). This should also be taken into consideration in education. It is ultimately the trainers' competence that decides to what extent these aspects can be utilized in training programmes.

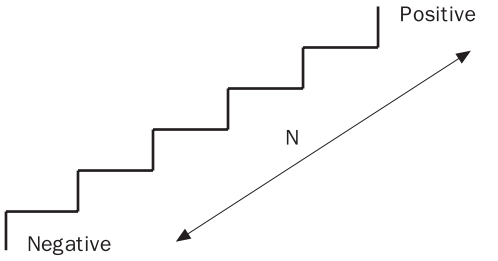
Intrinsic motivation in terms of Deci and intention (subjective norms, motivation to comply) in terms of Ajzen/TPB may also reflect on the different values users hold, on their view of life and on a host of social phenomena such as team/community spirit, organizational atmosphere and organizational/community culture. Good leadership skills and a healthy organizational culture tend to be important and necessary factors in the creation of a basis for security awareness, as they affect the achieving of intrinsic motivation and intention and also perceived usefulness in terms of TAM. Yet working conditions play a significant role in this respect, too. Labour dissatisfaction can result in unethical/immoral behaviour among employees (Bartol and Martin, 1994) and may ultimately give rise to various kinds of security threats.

2.2 How people may respond to approaches that increase awareness

Owing to non-uniform human behaviour with respect to different impulses (Locke, 1991), it is pivotal to outline and try to understand the different ways people respond to different methods and actions used to increase information security awareness. Since human responses are likely be multifarious, imprudent use of awareness actions may complicate the negative aspects of information security (which seems to be unknown to current research on security awareness). Some studies and theories, for example, adopt different stances towards commitment (Conner and Patterson, 1982; Taylor, 1995). Figure 1 demonstrates the widely agreed assumptions that there are different stages[11] (Conner and Patterson, 1982) – N = number of dynamic stages – symbolizing people's state of mind after the introduction of awareness activities. These stages constitute an implication relation, that there are people at every stage within practically every organization, and the success or failure of information security awareness correlates either with progress upwards (positive) or with regression downwards (negative). The terms positive and negative are conceived here from the perspective of a security administrator. From another point of view (e.g. a person seeing certain actions as totally wrong or deficient), resistance or hate may be a positive step as well.

On the positive side (see Figure 1), there is readjustment, co-operation, acceptance and internalization, among other things, whereas on the negative side there is repulsiveness or hate, even leading to different kinds of resistance. Even though this formula is only

Figure 1
How people may respond to awareness



an abstract framework developed out of a literature analysis (on qualitative empirical studies), it does help us to understand the need for careful planning, implementation and measurement. To give a practical example, with regard to planning and implementation, there seems to be no reason for assuming that internalization of security guidelines can be easily achieved straight away, i.e. there are no grounds to suppose that after a security awareness lesson people will all follow the guidelines at once. Taking this into account, user acceptance and internalization must be considered gradual processes and long-term goals.

It is not necessary to measure explicitly at what level people's attitudes may be. Explicit measurement of human attitude levels in this respect is in any case very difficult, and the advantage of any information gained is offset by the fact that it may vary depending on the person. Reliance on the results of deduction or induction, in connection with data of this kind may be questionable. The relevance of such empirical studies can be justified in the framework of qualitative research, however (as this kind of research would be qualitative). To give a practical example, some general tendencies with regard to the validity of the awareness approach in question can be perceived, and these results may assist us in trying to understand the different sorts of user behaviour we may have to face.

2.3 A reconsideration of methods and approaches for increasing awareness?

The contributions of McLean (1992) include "selling" information security to people through campaigns. This kind of action, campaigning, could in theory prove very useful in terms of security education, and provide a positive impetus for information security, since it may serve to maintain the importance of security in the eyes of employees. Campaigns have also been seen as good measures for improving attitudes (Peltonen, 1989) and it is reasonable to expect positive attitudes concerning security as well. On the other hand, as seen in Figure 1, security campaigns, like their political and advertising counterparts, may lead to unwanted results in terms of motivation and attitude, e.g. negative feelings, irritation, hate and various forms of resistance. Moreover, a selling process "where I sell and you buy" is not regarded as the equivalent to enrolment or commitment, since selling means persuading people to do something they would not do knowing all the facts (Senge, 1990, p. 218).

Hence, as with any other method, it should be used carefully, with controls, and not on its own. In the case of empirical-based controls, qualitative research should be used as a paradigm to be reflected by validating the success of the methods used.

Another practical method introduced by Perry (1985) is similar to campaigns. Its core lies in making information security an "in" topic (fashionable/everybody-wants-to-use-it) within an organization (Perry, 1985). It seems that campaigns and "in" topics can be used together in awareness programmes and that they may be good for providing incentives for end-users and for refreshing people's minds about the importance of these factors.

In addition, awareness involves education and training. Education should increase people's insight and answer the question "why" (it should increase motivation), while training should increase skills and competence (the ability part of performance, in terms of TPB/perceived behavioural control, which should have a positive effect by making compliance with security guidelines as easy task), and corresponds to an answer to the question "how". Since the "why" part is extremely important, employees should not be satisfied with answers such as "you just have to do it", "this is the rule", or "this is our policy" (traditional approaches). Their motivation and attitudes are not likely to be increased in this way.

Furthermore, from the viewpoint of behavioural theories (in section 2.1), it seems clear that a laissez-faire style of leadership and management attitude concerning human security matters, or the mere passing around of circulars (at worst circulars of a coercive nature) designed in the hope that the members of the organization will then strictly follow the given instructions (again traditional approaches), are also inapt and inapplicable procedures.

If the security guidelines based on these traditional approaches are not followed properly[12], this is due to the fact that such approaches are simply inadmissible. According to Hare (1997, p. 12) "the facts do not force us logically to make one moral judgement rather than another". In addition to moral norms, this is likely to be true of other norms or "ought" statements. Factual premises alone cannot imply norms ("ought" statements). If a computer is red (let us presume that this is a fact), it does not logically follow that we should (or should not) buy, prefer or use it only for this reason. Likewise, security guidelines that are presented in a factual/descriptive manner cannot logically serve as accomplishment-

oriented internal norms for end-users. We need to understand the normative nature of security guidelines, which will be considered in the next section.

Moreover, as we have seen, such traditional approaches may not gain support from motivational theories, either. In addition to this, the inadequacy of such "approaches" can be demonstrated by the theory of Cognitive Moral Development (CMD) of Kohlberg (1981)[13], which maintains that, in the case of moral matters, rational people are not satisfied with orders per se (without relevant explanation) or "because this is the rule".

3. Prescriptive awareness

The nature of a point of departure for information security awareness should be prescriptive, because information security guidelines are a kind of imperative, including, accomplishment-oriented commitment and internalization, for example. To explain this by a practical example, security people want end-users to internalize and follow given guidelines (prescriptive commitment) rather than to be aware of them but for some reason or other fail to apply them in reality. This seems to be the current problem: users often know the guidelines, but they fail to apply them correctly (Warman, 1992). The term "prescriptive" refers here to a situation where people see (internalize) a norm or guideline X as a matter which they are bound and obliged to follow. This kind of accomplishment-oriented commitment can be external or internal as a form of motivation. In terms of responsibility, the aforementioned obligation belongs to the category of role responsibility (e.g. one's duty as laid down by the firm), and hopefully to the moral responsibility category, too (one's moral concern to do the right thing), see Ladd (1982) on moral responsibility and Hart (1968) on other classes of responsibility. It is possible to achieve moral responsibility if the security actions of an organization are seen as morally acceptable and desirable in the eyes of the employees. In the long run, this obligation should be internal, coming from within the individual. External norms or guidelines, on the other hand, if they are so weighty and obligatory that they lead to prescriptive states, can cause greater risks in the form of negative implications (e.g. pressure or irritation may reduce work efficiency and even produce resistance or unethical or other unwanted behaviour).

The prescriptive nature of security guidelines means in practice that the mere provision of guidelines or education as such is not enough. Successful organizational awareness or education requires more actions than merely the giving of a set of rules (as is often the form of security guidelines). This is the case, since awareness or education, reflecting security guidelines, which consist of imperatives, has more to do with the internalization of needs than with other issues, e.g. facts generally[14]. One problem with security guidelines, however, is that only too often they are not justified in a relevant way, i.e. they are not justified as normative claims. This is definitely a problem, for guidelines should always be justified, since they are norms that include imperative forms that need argumentation and justification. In that way people's cognitive states can be changed by giving the reasons for particular guidelines (arguments and justifications), with the result that they may change their attitude and motivation towards the guidelines in the intended way. This kind of persuasive action, together with active participation, should constitute the basic use of security guidelines. When defining a wanted action, we usually give examples and additional information in an attempt to persuade the listeners to accept our evaluation and to adopt the kind of attitude we want them to display. Persuasion through communication (persuasive communication) has also been widely used and studied among behavioural scholars (Fishbein and Ajzen, 1975), albeit not with respect to information security, apart from an approach by Thomson and von Solms (1998).

Moreover, awareness with prescriptiveness as a goal has the characteristic of equifinality, meaning that the objectives may be achieved in different ways. This postulation is based on facts concerning human nature. Given that the behaviour of human nature cannot be formalized nor fully predetermined, all (awareness/education) methods are subjectively bounded in respect of situation, the instigator and the target person(s). Consequently, with regard to the division of the content of awareness, there are no structural cure-all solutions that always yield the desired results. After all, we are dealing with human nature (the subjective character of which is argued to be a fact by a mainstream human scientist (Koski, 1996). Thus, in every situation[15], we have a certain set of approaches which may work and some which may not.

4. A collection of approaches reflecting the requirements of prescriptiveness

The aforementioned use of norms with a kind of rhetorical discussion known as persuasion was first introduced by the philosopher Stevenson (1944) and later attracted the interest of behavioural scientists. In organizational security awareness, where the goal should be to achieve commitment, there is a need for this kind of rhetorical discussion.

Therefore it is reasonable to mention the use of the persuasion strategy influenced by Stevenson (1944), even though we do not agree with his theory of emotionalism, because it makes us realize that the mere description of security guidelines possibly with some reinforcement actions, e.g. punishment[16] (other reinforcement actions are positive reinforcement, negative reinforcement, extinction) is not enough. Negative reinforcement (NF) differs from punishment in that: it encourages or increases desirable behaviour, while the objective of punishment is to reduce undesirable behaviour; punishment is carried out after undesirable behaviour, i.e. actions against security policy (at the abstract level) or security guidelines (at the operative level), whereas NF is applied before a violation (Bartol and Martin, 1994). Deterrents with respect to security are examples of negative reinforcement actions.

For the reasons outlined here, the use of persuasion in security education is recommended. In addition to the occasional use of a reward and sanctions system, there are certain persuasion approaches reflecting motivational factors that security education can use and pursue to ensure that listeners internalize the principles of given guidelines. The possible usable persuasion approaches that relate to people's behaviour, in addition to the aspects mentioned in section 2.1, are summarised in Table III.

Attitude is particularly important in terms of TPB and TAM/behavioural intention. The sign "+" means that the approach in question (e.g. appealing to emotions) is seen to satisfy a certain theory or part of a theory (e.g. intrinsic motivation), while the sign "–" means the opposite. "Pave the way" means that, although the approach does lead to intrinsic motivation or positive attitudes towards security guidelines per se, the approach may facilitate the achievement of intrinsic motivation/attitudes or may even be a precondition for achieving these. Subjective norms in terms of TPB, consisting of normative beliefs (coming from others) and motivation, are not considered in the table, since normative beliefs can in theory lie behind any such persuasion strategy, and motivation is considered here in terms of intrinsic motivation. Also, as mentioned above, ease of use in terms of TAM and CBPF in terms of TPB are best taken care of by technical education and are thus not considered with respect to persuasion. The principles are reasoned as follows:

Table III
Some practical approaches and presuppositions regarding their possibilities with respect to motivation

Practical approaches/ Principles	Intrinsic motivation	Attitude
Logic	Pave the way	Pave the way
Morals and ethics	+	+
Rationality	Pave the way	+
Emotions	+	+
Sanctions, pressure	–	+
Feeling of security	+	+
Well-being	+	+

- *Logic.* All actions should be logical. Do not act inconsistently. If, for example, a superior argues for relevance of the universality principle and then tries to justify compliance with security guidelines by appealing to this principle, that superior cannot later logically plead for an action that violates this principle (without providing any persuasive reasons for why the universality principle is not relevant in this particular situation).
- *Emotions*. Emotions are an integral part of thinking and rational decision making. When people are confronted with a set of choices, emotional learning (past experiences) streamlines their decisions by eliminating some options and highlighting others (Goleman, 1995). Consequently, security measures should aim at provoking emotions and appealing to them in order to affect attitudes and motivation in a positive manner.
- *Morals and ethics*. Morals strongly guide human behaviour. Smith (1984), among others, has even argued that it is more intelligible to act for moral reasons than for non-moral ones, although this view has been criticised (Dancy, 1994), on the grounds that moral, or justified, reasons do not imply motivation per se (since Dancy argues that one may see non-moral reasons as intelligible as well). More persuasively, R.M. Hare (1963) sees that the moral aspect overrides all other concerns. Thus, if killing an innocent

person is regarded as immoral, we may not – and should not – kill innocent persons, regardless of the non-moral concerns related to the issue, e.g. financial gain. Security norms, at least those imposed by legislation, are – hopefully – founded on moral and ethical notions (this is not always so in practice, however). They are – hopefully – arrived at by means of ethical analyses (carried out by conceptual analysis) and should correspond to a desirable state-of-affairs. Electrical break-ins (nowadays often referred to as hacking), are (or should be?) covered by legislation because it seems to be wrong (in a general sense) to gain unauthorized access to computers or information systems. But why does it seem to be morally wrong to do so? Using the principle of universality, which plays in important role in Kantian, Christian, Confucian and universal prescriptivism, according to Hare, or Rawls' (1972) justice by fairness in terms of the "veil of ignorance", for example, we could ask: "What if everybody were to indulge in hacking?" We would most probably not want anyone to break into our computer systems, or our houses as we feel that life in such a society would be very uncomfortable (and we postulate that this is one reason why hacking should be regulated as a criminal activity by legislation). Although there may be a moral dimension behind security activities (although this does not mean that security activities are right per se), it is commonly agreed by computer ethicists that people often fail to realize it (Kesar and Rogerson, 1997). As a result, they do not apply their moral notions to the area of computing, and an important stimulus (human morality/moral responsibility) is lost from the security point of view. If people were to understand the ethical dimensions of security procedures (such as inadequate maintenance of passwords) and the possible morally negative consequences of such negligence, they would probably be more likely to follow the instructions. Different ethical theories should be used for this purpose.

- *Well-being*. Negligence of security measures and weak security may threaten the well-being of individuals, companies and societies. Therefore, users should be made aware of such a threat to their well-being and how adherence to security guidelines would prevent this from happening. This differs from morals and ethics in the respect that loss of well-being may have non-moral consequences.
- *Feeling of security*. Safety needs (the desire to feel safe and secure, and free from threats to our existence) rank high among our needs, according to Maslow (1954). Even though Maslow's theory has been criticised, mainly due to the lack of proof for its hierarchy of needs, the fact remains that "needs are the fundamental reason why people act and thus are essential to a full understanding of motivation" (Locke, 1991, p. 290). Although violations in terms of information security would not endanger people's lives directly (other than in a hospital environment, for example), it is reasonable to assume that people will still want to achieve and maintain a feeling of security through adherence to security procedures – given that such a need can be pointed out or awakened. Like morals and ethics, computing may be a blind spot for this, where users may not themselves recognize the possible jeopardy, such as the invasion of their informational privacy, or the deletion, modification or unauthorized use of their information.
- *Rationality*. This involves the rational presentation of factual, descriptive reasons for actions. People are rational (at least in some respects), and they therefore demand rational explanations. The following issues, for example, can be addressed thoroughly according to the requirements of rationality: What are the implications of weak security for the company and the employees? Why is it rational to follow security guidelines? Why is it irrational not to follow security guidelines or pay attention to security?

Attention to these various points requires logical consistency, so that conflicts or inconsistencies with respect to persuasive actions cannot be tolerated (see Stevenson, 1944 and the notion of moral management)[17]. In addition, when appealing to morality, emotions, etc., IT professionals cannot simply pay lip service and apply a double standard of morality, as such a procedure is likely to have negative consequences, at least in the long run. It is very important that the people responsible for raising security awareness should regard the methods for doing so as positive and truly right, and should be capable of justifying them if challenged. This is a necessary point of departure for the persuasion method.

5. Conclusions

The creation of an information security awareness programme as a means of

minimizing end-user errors regarding security guidelines requires a systematic approach. This study started with a division of the doctrines of awareness into framework and content parts. The first part, the framework, should be developed in a systematic and structural manner, with the help of appropriate standards etc.

In as far as end-user internalization of the security guidelines/procedures is the objective, the content part of the awareness programme must also come under serious consideration. In that respect, the behavioural framework is depicted here and current approaches to awareness are analysed from the point of view of behavioural theories.

The difference between descriptive and prescriptive (factual/normative, respectively) is presented and the need for and relevance of a prescriptive point of departure is justified. It is argued that all approaches affecting the behaviour of the user (increasing awareness, etc) should, in order to be effective, satisfy the requirements of behavioural theories and provide answers for end-users, explaining (or letting them observe) why they should follow security guidelines. In this respect, a set of persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions is set out.

The use of such a persuasion strategy should not be based on a double standard of morality, however, but should stand up to closer scrutiny, as this is a necessary condition for giving of any strategy for increasing awareness a solid basis and for achieving user commitment.

The main limitations of this work lie in the research method used (conceptual analysis). Empirical studies are now needed to consider the validity of the persuasion framework presented here.

I have benefited from the expertise of many people while preparing the early versions of this paper. These persons include Dr Veli Verronen at the Department of Social Sciences and Philosophy, University of Jyväskylä, assistant professor Veikko Launis at the Department of Philosophy, University of Turku, and Professor Juhani Iivari and Mr Pekka Abrahamsson at the Department of Information Processing Science, University of Oulu. Mr Malcolm Hicks has corrected my English grammar.

Notes

1 According to Senge (1990 s. 219) commitment to something means that one wants it and will make it happen.

2 Swain and Guttman (1983), for example, divide human faults into four groups: errors of omission, errors of commission, sequence errors and timing errors. The most common security-related errors among end-users are: errors of omission, i.e. failure to do X; and errors of commission, in other words, incorrect execution of a procedure. Other kinds of fault are more common among IT/computer professionals than non-professional end-users, but a closer perusal of these errors falls outside the scope of the present paper.

3 Using the distinction between tacit and explicit knowledge originally proposed by Polanyi (1966). Tacit knowledge is personal and context-specific (e.g. riding a bike), and is hence difficult to formulate or communicate, while explicit knowledge is transmittable through formal or systematic expression.

4 Probably because its formal nature allows an easy application of the traditional view of engineering/computer science.

5 M/B denotes reflected research disciplines, and particularly whether the authors have reflected some particular motivational/behavioural theories, while RM refers to the research methods used. The classification of research methods presented by Järvinen (1997) is used here. CA stands for conceptual analysis (e.g. attempts are made to apply the principles of motivational theories to security questions and/or awareness methods/principles are validated by means of existing behavioural theories). AE, referring to the Authors' Experience (e.g. "I believe", "I feel" argumentation) is not included in any research classification, since "I believe" per se is not scientifically adequate to provide validation (e.g. Chalmers, 1982).

6 The term descriptive is not the same as descriptivism in the area of the philosophy of science in the sense advocated by Reid, Kirschhoff, states that theories do not explain phenomena, but rather try to describe them, i.e. science does not find out what or why, but asks how. The term descriptive is used here in its moral, philosophical meaning, in a similar sense to that proposed by R.M Hare (1952), to distinguish a situation as being non-prescriptive – see Hare (1997, p. 42). Explicitly, descriptive refers to a (conscious/unconscious) view that purely descriptive statements such as facts can imply norms.

7 Even though there are many kinds of end-users in organizations, the different categories are not distinguished here. The term end-user is used to refer broadly to an employee using a computer for certain organizational purposes, given that this use is covered by (information) security policy and regulated by certain information security guidelines.

8 Ability refers to an individual's capability to accomplish certain tasks. It is usually stable and influences direction and behaviour, but does not finely tune behaviour. Motivation, in turn, finely tunes behaviour. Moreover, motivation depends on factors such as needs and stimuli.

9 This does not mean that decision making concerning security techniques should be on the end-users' shoulders. It simply means that end-users should have the feeling (as required by intrinsic motivation) that their preferences have been considered adequately and that they should see security activities as being entirely rational and clearly justified (in their own eyes).

10 Under such circumstances people are likely to be more committed to security measures and less likely to resist them.

11 Research seems to reach different views on the number of stages (Conner and Patterson, 1982; Taylor, 1995), and therefore the symbol N is used to describe them. Agreement over the number of possible stages and their names is

irrelevant for the present discussion, however.

12 Even the simplest security procedure demanded by security guidelines, such as the correct use of a password, is often ignored.

13 In this paper we are especially interested in the order of orders/punishment, legal and moral, as motivators. In his theory, punishment as a motivator is the lowest level (the Stage of Punishment and Obedience) and complying with conventional norms (those set by society and/or acquired through upbringing) is the third stage. The highest stage of moral development, however, is achieved when actions are based on moral responsibility. Kohlberg in particular argues that universalizable principles represent the peak of moral development. This should help us to understand why people need explanations rather than merely rules and the threat of punishment.

14 On the other hand, people may not see security guidelines as "factual" matters, evidence of which has "proved to be factual/rational".

15 A strategy of awareness is a very organizationally dependent matter, requiring knowledge of the social culture of the organization in question. For example, in the case of military organizations, which are likely to be bureaucratic in terms of organizational structure, even pure order-based strategies may work well, whereas they are likely to be insufficient (even constituting negative stimuli) in "task force" types of organizations.

16 Sanctions relating to the non-observance of guidelines, even though they may be necessary, are often external to a person. Therefore, they may have the negative consequences common to extrinsic motivation (described earlier) and are effective as long as the threat of punishment is valid. In addition, the long-term effects of both punishment and negative reinforcement are often recognized as being negative (Bartol and Martin, 1994). Anyhow, if people understand the reasons behind the norms, they may understand better the possible need for punishment. This latter situation, including the giving of rewards, may lead to the combining of extrinsic and intrinsic motivation in a positive way.

17 According to Carrol (1987), there are several types of managerial ethics: immoral (can we make money with this action, decision, etc., while other considerations matter little, if at all); amoral (ignores ethical considerations; can we make money with this action, or decision within the letter of the law?); and moral management (pursue business objectives which involve simultaneously making a profit and engaging in legal and ethical behaviour; is this action or decision fair to us and all parties involved?).

References

Adams, D.A., Nelson, R.R. and Todd, P.A. (1992), "Perceived usefulness, easy of use, and usage of information technology: a replication", *MIS Quarterly*, Vol. 16 No. 2, pp. 227-47.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50, pp. 179-211.

Bartol, K.M. and Martin, D.C. (1994), *Management*, Second international edition, McGraw-Hill, New York, NY.

Baskerville, R. (1989), "Logical controls specification: an approach to information system security", in Klein, H. and Kumar, K. (Eds), *Systems Development for Human Progress*, North-Holland, Amsterdam.

Carrol, A.B. (1987), "In search of the moral manager", *Business Horizons*, March-April, p. 8.

Ceraolo, J.P. (1996), "Penetration testing through social engineering", *Information Systems Security*, Vol. 4 No. 4, Winter.

Chalmers, A.F. (1982), *What Is the Thing Called Science?* Second edition, Open University Press, Milton Keynes.

Chau, P. (1996), "An empirical assessment of a modified technology acceptance model", *Journal of Management Information Systems*, Vol. 13 No. 2, pp. 185-205.

Conner, D.L. and Patterson, R.W. (1982), "Building commitment to organizational change", *Training and Development Journal*, April, pp. 18-30.

Dancy, J. (1994), "Why there is really no such things as the theory of motivation", *Proceedings of the Aristotelian Society*.

Davis, F. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, September, pp. 319-40.

Deci, E.L. (1975), *Intrinsic Motivation*, Plenum Press. New York, NY.

Deci, E.L. and Ryan, R.M. (1985), *Intrinsic Motivation and Self-determination in Human Behaviour*, Plenum Press, New York, NY.

Fishbein, M. and Ajzen, I. (1975), *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, MA.

Goleman, D. (1995), *Emotional Intelligence*, Bantam Books, New York, NY.

Goodhue, D.L. and Straub, D.W. (1989), "Security concerns of system users: a proposed study of user perceptions of the adequacy of security measures", *Proceedings of the 21st Hawaii International Conference on System Science (HICSS)*, Kona, HA, January.

Hare, R.M. (1952), *The Language of Morals*, Clarendon Press, Oxford.

Hare, R.M. (1963), *Freedom and Reason*, Oxford University Press, Reprinted in 20th century Ethical theory, in Cahn, S.M. and Haber, J.G. (Eds), *R.M Hare: A Moral Argument*, 1995, Prentice-Hall, Englewood Cliffs, NJ.

Hare, R.M. (1997), *Sorting Out Ethics*, Oxford University Press, Oxford.

Hart, H.L.A. (1968), *Responsibility and Retribution*, Oxford University Press, Oxford.

Hoffer, J.A. and Straub, D.W. (1989), "The 9 to 5 underground: are you policing computer crimes?", *Sloan Management Review*, Vol. 30 No. 4, Summer.

Igbaria, M. and Zinatelli, N. (1997), "Personal computing acceptance factors in small firms: a structural equation model", *MIS Quarterly*, Vol. 21 No. 3.

Järvinen, P. (1997), "The new classification of research approaches", *The IFIP Pink Summary – 35 Years of IFIP*, Edited by Zemanek, H., IFIP, Laxenburg.

Kesar, S. and Rogerson, S. (1997), "Developing ethical practices to minimise computer misuse", *Proceedings of International IEEE Symposium on Technology and Society: "Technology and Society at a Time of Sweeping Change"*, IEEE Computer Society Press, Piscataway, NJ.

Kohlberg, L. (1981), *The Philosophy of Moral Development*, San Francisco, CA.

Koski, L. (1996), "The truth, the quality, and the interpretation", in Julkunen, K. (Ed.), *Qualitative Methodology in Educational Research*, University of Joensuu, Bulletins of the Faculty of Education, No. 60, Joensuu, Finland.

Ladd, J. (1982), "Collective and individual moral responsibility in engineering: some questions", *IEEE Technology and Society*, Vol. 1 No. 2, pp. 3-10.

Locke, E.A. (1991), "The motivation sequence, the motivation hub, and the motivation core", *Organizational Behavior and Human Decision Processes*, Vol. 50, pp. 288-99.

Maslow, A.H. (1954), *Motivation and Personality*, Harper & Row, New York, NY.

Mathieson, K. (1991), "Predicting user intentions: comparing the technology acceptance model with the theory of planned behaviour", *Information System Research*, Vol. 3 No. 2, pp. 173-91.

McLean, K. (1992), "Information security awareness – selling the cause", *Proceedings of the IFIP TC11/Sec'92*, 27-29 May, Singapore.

Morwood, G. (1998), "Business continuity: awareness and training programmes", *Information Management & Computer Security*, Vol. 6 No. 1, pp. 28-32.

(The) NIST Handbook (1995), *An Introduction to Computer Security*, NIST special publications in October.

NIST (1998), Information Technology Security Training Requirements: A Role-and Performance-Based Model (supersedes NIST Spec. Pub.500-172), SP 800-16, March.

Parker, D.B. (1998), *Fighting Computer Crime – A New Framework for Protecting Information*, Wiley Computer Publishing, New York, NY.

Peltonen, M. (1989), *Management in the 1990s*, Aavaranta Serie. No. 14, (in Finnish) Otava, Keuruu, Finland.

Perry, W.E. (1985), *Management Strategies for Computer Security*, Butterworth Publisher, Boston, MA.

Polanyi, M. (1966), *The Tacit Dimension*, Routledge & Kegan Paul, London.

Rawls, J.A. (1972), *A Theory of Justice*, Oxford University Press, Oxford.

Senge, P.M. (1990), *The Fifth Discipline: The Art and Practice of the Learning Organization*, Doubleday Currency, New York, NY.

Siponen, M.T. and Kajava, J. (1998), "Ontology of organizational IT security awareness. From theoretical foundations to practical framework", Third International Workshop on Enterprise Security, *IEEE 7th International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WET ICE '98)*, IEEE Computer Society Press, Los Alamitos, CA.

Smith, M. (1984), *The Moral Problem*, Blackwell, Oxford.

Spruit, M.E.M. (1998), "Competing against human failing. 15th IFIP World Computer Congress, 'The Global Information Society on the way to the next millennium'", *Proceedings of the SEC'98*, TC11, Vienna.

Spurling, P. (1995), "Promoting security awareness and commitment", *Information Management and Computer Security*, Vol. 3 No. 2, pp. 20-6.

SSE-CMM (1998a), The Model, v2.0, http://www.sse-cmm.org.

SSE-CMM (1998b), The Appraisal Method, v2.0. http://www.sse-cmm.org.

Stevenson, C.L. (1944), *Ethics and Language*, New Haven, CT.

Straub, D.W. (1990), "Effective IS security: an empirical study", *Information System Research*, Vol. 1 No. 2, June, pp. 255-77.

Straub, D., Carson, P. and Jones, E. (1992), "Deterring highly motivated computer abuses: a field experiment in computer security", *Proceedings of the IFIP TC11/Sec'92, Security and Control: From Small Systems to Large*, Singapore, 27-29 May.

Straub, D.W., Keil. M. and Brenner, W. (1997), "Testing the technology acceptance model across cultures: a three country study", *Information & Management*, Vol. 31 No. 1, November, pp. 1-11.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*, Vol. 22 No. 4, p. 441-64.

Swain, A. and Guttman, H. (1983), *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Nuclear Regulatory Commission, Washington, DC.

Taylor, W.A. (1995), "Senior executives and ISO 9000: attitudes, behaviours and commitment", *International Journal of Quality & Reliability Management*, Vol. 22 No. 4, pp. 40-57.

Telanne, M. (1997), Intrinsic Motivation – Some Theoretical and Empirical Observations, Research of Management (Hallinnon tutkimus), No. 3:237-245, in Finnish.

Thomson, M.E. and von Solms, R. (1997), "An effective information security awareness program for industry", *Proceedings of the WG 11.2 and WG 11.1 of the TC11 IFIP*.

Thomson, M.E. and von Solms, R. (1998), "Information security awareness: educating our users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-73.

Warman, A.R. (1992), "Organizational computer security policy: the reality", *European Journal of Information Systems*, Vol. 1 No. 5, pp. 305-10.