Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice

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

Keywords
Information systems, Security, Education

Abstract
Even though the human component has been recognized to have a crucial role in information systems (IS) security, the human issues have not received much attention. Recently a few approaches aimed at minimizing human-related faults in the area of IS security have been put forward. This paper analyses different approaches aimed at minimizing user-related faults. The existing approaches will be analysed from the viewpoint of their theoretical background, the research approaches employed, the research objectives and the organizational role of IS security. As a result, a new taxonomy, a comparison and critical analyses of the strengths and weaknesses of state-of-the-art approaches shall be presented. Moreover, several issues that future research should explore and practitioners should consider when applying the results of the existing research are suggested.

The author would like to thank Mr Timo Mäntyvaara for checking my grammar. The author would also like to thank the OWLA-project for financial support (http://www.tol.oulu.fi/wise/index.html).

Information Management & Computer Security
8/5 [2000] 197–209

[ISSN 0968-5227]

1. Introduction

Many people in the security business regard the human factor as the weakest link in security solutions (e.g. Perry, 1985; Angel, 1993). Whether this is true does not take away the widely agreed view that in any case the human factor plays an important role in security solutions (e.g. Anderson, 1993; Bishop *et al.,* 1997, p. 57; Spruit, 1998; Straub, 1990; Straub and Welke, 1998). This can be justified by stating that a security technique, no matter how effectual, can be misused or misinterpreted by users, thereby losing its usefulness.

Taking this as a point of departure, several different approaches to coping with this human issue, with disparate viewpoints, have been introduced by information security scholars. Even though the approaches are different, they all seem to have the same mission statement: to increase the intended use of security solutions (whatever the techniques or procedures). These approaches to maximize the intended use of security solutions shall be referred to as "human/user-related faults".

In order to understand the different approaches, they can be classified into two categories as follows. The first category encompasses contributions which try to affect the users' behaviour by other means than punishment. These studies may not deny the relevance of punishment, but they propose other means of affecting the behaviour of the user, such as increasing the motivation of the users. Equally, the punishment community may not deny the role of the other means. For example, according to Straub and Widom (1984), who belong to the punishment community, (professional) ethics can function as a protection mechanism. In the case of the second category, the problem is approached by introducing external deterrence such as punishment activities. A taxonomy of the existing approaches is described in Table I.

With regard to the first category, the most commonly used approaches are information security awareness, education and training. Other approaches that have been presented with this objective include "user-centred security" by Zurko and Simon (1996), and a proposal by Spruit (1998). There are also other courses of action related to the issue in question, which however have only been developed to the level of principle. These include, among other things, the principles of ease of safe use (e.g. Saltzer and Schroeder, 1975) and transparency.

Within the first category, the studies can be further divided into two classes (Table I – the affected area). The first set of approaches attempt to affect the human component per se, whereas the other class encompasses approaches contributing to security-related products covering, for instance, issues that have to do with user-friendliness. Thus, the concept of "awareness" belongs to the first (human component) part, while "user-centered security", attempting to increase the usability of different products, belongs to the product part. Even though the importance of the area of user-related faults is a fact, there are no critical studies available that explore the applicability and usability, as well as the strengths and weaknesses of the different approaches. This kind of effort would be worthwhile for several reasons. First, any theories should be analysed critically, which is an aim of science – the self-corrective research method is widely agreed as a basic "method" of science[1] (Niiniluoto, 1990, 1999; Popper, 1992) – and shall be used herein: critique plays an essential role by forcing us to prove our ideas and our logical reasoning. The information resulting from the analysis should be relevant for practitioners as well. Consider cryptography, for example. Would practitioners prefer to apply proposals that have not been tested/considered critically or proposals that have been critically analysed by

Table I
A taxonomy of current research

Category	Affected area	Current research	Main proposals
Category 1: Non-punishment community	Human component	McLean (1992)	Campaigning
		Perry (1985)	Make security an "in" topic
		NIST (1995; 1998)	A framework for awareness
		Thomson and von Solms (1997)	A framework for awareness
		Thomson and von Solms (1998)	A framework for awareness
		Spurling (1995)	The importance of commitment
		Siponen (2000a)	Understanding of factual-normative dualism; application of the theories of intrinsic motivation, (e.g. Deci, 1975) reasoned action (Fishbein and Ajzen, 1975), planned behaviour (e.g. Ajzen, 1991), technology acceptance model (Davis, 1989); a persuasion strategy
		Spruit (1998)	All-encompassing security guidelines are difficult to write; incident analysis; clarification of human failures; suggestions for avoiding human failures
	Products	Zurko and Simon (1996)	Make security products easy to use
Category 2: Punishment/ deterrence community		Straub (1990)	Punishment as deterrence is relevant
		Straub *et al.* (1992)	
		Parker (1981, 1998)	Punishment as deterrence is relevant

the research community? Second, it is useful for practitioners, researchers and educators (e.g. at universities) to know the theoretical foundations (or recognize the lack of theoretical foundations) of the different studies. Finally, comparative papers should generally be relevant for practitioners by giving them a comparative view of the available approaches. Practitioners may not have much time to explore the literature jungle. This paper addresses the aforementioned issues by analysing the strengths and weaknesses as well as various fundamental assumptions of the different methods of studying user-related faults. This research objective will be achieved by analysing the existing approaches from the viewpoint of the underpinning theoretical background, the research approaches employed, the research objectives and the organizational role of IS security. Conceptual analysis in terms of Järvinen (1997; 2000) is used as the main research method to achieve these results. Although this paper offers some criticism, we would like to state that each of the authors discussed herein has made significant contributions to this area. Moreover, the objective of this study is not to refute the analysed approaches, but rather to compare and to point out some possible weaknesses in order to improve the approaches.

The scope of this paper is limited to the end-user perspective. Other discussed human-related issues including education and awareness at the managerial level, the means of developing software development methods for this purpose, as well as managerial and leadership approaches are beyond the scope of this paper.

Awareness approaches including McLean (1992), NIST (1995; 1998) and Thomson and von Solms (1997; 1998) are discussed by Siponen (2000a) and are therefore not addressed in this study. There are also considerations of whether "ethics" (Kowalski, 1990; Leiwo and Heikkuri, 1998a, 1998b; Siponen, 2000b) and the codes of ethics (Harrington, 1996) can be used to minimize human-related faults. However, there is no space to engage in a debate concerning the relevance of such approaches. An earlier version of this paper is presented in Siponen (1999).

This study is organized as follows. In the second section, the framework for the analysis is presented. In the third section, ease of safe use and transparency are considered. In section four, an exposition of the user-centred security doctrine together with some criticism aimed at it will be presented. The fifth section focuses on organizational psychology and the incident analysis approach, including some criticism. In the sixth section the foundations of deterrence (punishment) will be considered. The seventh section summarises the key issues of the study, and finally a list of references will be presented.

2. Framework for the analysis

The framework for the analysis (see Table II) is as follows.

Research approaches employed

The classification of research approaches presented by Järvinen (1997; 2000) is used here. Two research approaches were found: conceptual analysis and empirical research.

Logical strengths and weaknesses refer to aspects that can be found by conceptual analysis. In other words, the strengths and weaknesses are herein issues that can be rationally explained. What does this really mean? Let us presume that the weaknesses of a theory X are widely known. Let us also presume that a method Y to minimize user-related faults is based on this theory and the author is unaware of the weaknesses of theory X. It can be claimed that method Y has a logical weakness: it is built on "an error theory", the result being that we cannot be sure of whether the method is adequate in practice.

Reference disciplines reflected

The reference disciplines are marked only if the authors have indicated them explicitly or used and referred to some discipline (e.g. psychological literature).

The views about the organizational role of IS security (ISS) are distinguished into technical, socio-technical and social (Iivari and Kerola, 1983; Iivari and Hirschheim, 1996). The technical view holds that the emphasis of IS (security) development lies in technical matters. The social school emphasises the development of organizational systems before technical issues. The socio-technical perspective is between these two, viewing technical and organizational systems as equally important.

The research objectives can be divided into: means-end oriented; interpretive; and critical, set forth by Chua (1986). This separation is also used by Iivari (1991) and Iivari *et al.* (1998) for comparing IS development methods, as well as by Siponen (2000c) for analysing the approaches to designing secure ISs.

Table II
Framework for the analysis

Framework for the analysis	Aims
Research approaches used	To find out what research methods are used and preferred to develop solutions
Logical strengths and weaknesses	To find out the strengths and weaknesses of the approaches
Reference disciplines	To find out what the theoretical backgrounds of the approaches are
Organizational role of IS security	To find out whether the role is technical, socio-technical or social
Research objectives	To find out whether the research objectives are: means-oriented; interpretive; or critical

3. Ease of safe use and transparency

The central thesis: ease of safe use

Ease of safe use is first presented by Saltzer and Schroeder (1975) among the eight design principles for constructing secure computer systems. According to the ease of safe use, the security mechanism should be as easy to use as possible, and the presence of a security mechanism should not cause any notable difficulties to the use of computers.

The theoretical background of ease of safe use

Although Saltzer and Schroeder (1975) merely put forth a principle (based on their experience and knowledge), their idea (without their knowing it in 1975) gets support from behavioural science. The technology acceptance model by Davis (1989), the theory of reasoned actions by Fishbein and Ajzen (1975) and the theory of planned behaviour by Ajzen (1991) all recognize ease of use as an important factor affecting human behaviour. However, a question of what is "ease of (safe) use" has not been considered in security literature; in other words, what makes a security solution or a method as easy to use as possible. We believe that qualitative research approach would be relevant to address this question.

The central thesis of transparency

Transparency relates closely to the principle of ease of safe use, as it makes security techniques invisible to the user. Therefore, the strength of this principle is that it should make the use of security techniques and adherence to procedures very easy.

Weaknesses of transparency

The introduction of transparency may bring about some weaknesses, however. First, invisibility may increase a value vacuum with respect to computer technology[2]. A second, and perhaps more crucial weakness from security point of view is that it may increase the likelihood of the occurrence of certain security weaknesses. This may be the case since people may take security as granted and may easily neglect or misuse possible forthcoming security mechanisms that are more visible or difficult to use. Abuses may also not be viewed and reported as easily as before.

The organizational role of IS security, the research objective and research approach

The view of Saltzer and Schroeder (1975) concerning the organizational role of IS security is more technical than socio-technical. Their main concern lies in the

technical solutions. The objective of their research is also means-oriented. They provide principles in order to produce knowledge for achieving certain concrete goals. Their research method is conceptual analysis.

4. User-centred security

The central thesis: usability of security solutions and procedures

User-centred security (hereafter referred to as UCS) stands for "security models, mechanism, systems, or software that have usability as a primary motivation or goal". The main areas, according to Zurko and Simon (1996), can be classified into the following three categories:

1 Applying usability testing and techniques to secure systems.
2 Developing security models and mechanisms for user-friendly systems (e.g. groupware).
3 Considering user needs as a primary design goal at the start of secure system development.

In a sense the aim of UCS is not original. As pointed out earlier in this article, as early as 1975, Saltzer and Schroeder (1975) set out psychological acceptability as one of the design principles of secure systems. However, although we may see this as a persuasive goal, not much work has been done to study this further[3] (while other principles, such as the so-called least privilege principle introduced by Saltzer and Schroeder, have received more attention). The authors of UCS offer some reasons to explain this negligence. First, some may see usability and security as conflicting components (secure systems have traditionally been difficult to use)[4]. Second, most development and research in secure systems has strong roots in the military. The atmosphere in the military sets rather different qualifications for ease of safe use (Zurko and Simon, 1996). However, in the information society of today security is an issue that concerns a much wider field than just the military. Therefore, the usability issues are relevant provided that users want to use the solutions (cf. Mathieson, 1991).

The theoretical background

UCS does not mention any theories. The theoretical foundations of the usability claims can be traced back to TRA (Fishbein and Ajzen, 1975) and TAM (Davis, 1989), which have been discussed earlier.

The organizational role of IS security, the research objective and research approach

The objectives of UCS research are means-oriented. First and foremost, the main objective of UCS is to achieve certain ends, namely to develop security models, mechanism, systems, and software that are usable (e.g. easy to use). The UCS views the organizational role of IS security as social. This is concluded since the primary purpose of UCS is usability (and other qualities come after that). The used research method is conceptual analysis.

Weaknesses and open questions

UCS is confronted with the following three weaknesses:

The objective of UCS are approaches "that enable users to choose and use the protection they want, that matches their intuition about security and privacy, and that supports the policies that teams and organizations need and use to get their work done" (Zurko and Simon, 1996). This statement involves a source of conflict that may result in its inapplicability to practical work (at the organizational level) as such. The conflict is that the policies of organizations may require quite different activities than the solution that the users would choose. To give a precise example, security people are not likely to want users to be able to choose the protection they want – although in some sense security people would be the beneficiaries of such an arrangement in the long run (e.g. user satisfaction may be necessary for achieving "users' internal" commitment towards security policy – consider for example intrinsic motivation by Deci, 1975; Deci and Ryan, 1980; 1985). Thus, if the preferences of the users and the requirements of the organization are in conflict, what should we do? The doctrine of UCS does not state how to compromise the requirements of users and security persons, for example. Moreover, UCS does not put forth any methods for capturing or modelling such requirements (some information systems development methods help in capturing and modelling such requirements).

Second, the scheme of Zurko and Simon (1996) forgets an issue that has to be taken into account in every practical solution, namely politics. Politics can be divided into desirability and feasibility (Kukathas and Pettit, 1990). In terms of politics, the model of UCS takes into consideration the desirability component. However, UCS, at least currently, does not take any measures towards establishing feasibility, which is an important part of politics as well. The feasibility issues referred to here include

questions such as "what is a feasible solution?" This also involves, for instance, financial aspects. Feasibility plays an important role in all security solutions – a fact that is neglected in Zurko and Simon's scheme. To give an example of this, as far as organizations are concerned, all user preferences may not override financial concerns.

Third, usability (as well as transparency), when used as the only method for solving security problems that are due to mistakes by end users, might implicate unawareness, which may be a possible cause for security breaches. There are a lot of threats even to the occasional net-surfer (and threats can be a real risk to a person who is unaware of them). For example, consider WWW-impersonation, where some malicious party sets up a Web page, perhaps using IP forgery, pretending to be a service provider of some commercial service.

5. Organizational psychology and incident analysis

The basic assumption of OPIA

Spruit (1998) has introduced the organizational psychology and incident analysis (hereafter OPIA) approach, which argues that human errors can be overcome only by understanding human behaviour. According to OPIA, the traditional tendency to focus on security means and motivation does not work well. Particularly, Spruit sees that the solving of problems by strengthening the security measures and increasing so-called security awareness can yield only marginal improvements. This claim is based on the view that current research on awareness does not take into account the concept of human behaviour, although current research such as Spurling (1995), NIST (1998) and Thomson and von Solms (1998) does take it into account. In fact, considering the work of the awareness community, a more proper term instead of "awareness" would be "commitment". Nevertheless, the view of the awareness community is supported by studies of behavioural scientists. Behavioural scientists have discovered that lack of motivation relates to misbehaviour (e.g. Vardi and Weiner, 1996).

Thesis 1

The OPIA thesis presents two kinds of behaviour as the relevant theoretical framework with respect to human errors cited from Bernstein *et al.* (1994) and Robbins (1998):

- unconscious behaviour;
- conscious behaviour.

Unconscious behaviour is characterized by automatic actions that are the result of a long-term learning period (e.g. walking) and that are rather reliable. Unconscious behaviour can be changed in two ways. First, by making the unconscious behaviour conscious (in other words, to change behaviour in the same way as other conscious behaviour). Second, by thorough modification of the environment in such a way that the required behaviour is either the most logical or the only possibility available.

Spruit (1998) does not follow any particular theory, but rather bases his arguments on general textbooks on psychology/organizational behaviour, such as Bernstein *et al.* (1994) and Robbins (1998), respectively.

Weaknesses of thesis 1

The aforementioned classification is not totally perfect since human behaviour cannot be fully captured by these two conceptions, as for instance the issue of the weakness of the will is not included. As a matter of fact, the weakness of the will is likely to be an important issue with respect to human error (e.g. Mortimore, 1971), as we shall see.

Another way to influence behaviour is to enforce behaviour through modification of the environment. However, this may introduce a weakness, since modification of the environment as a means of influencing behaviour may also implicate negative consequences. Thus, modification of the environment in the above sense may cause negative impulses: at least it should not increase motivation and user commitment (cf. Deci and Ryan, 1980).

Thesis 2 and the possible theoretical foundations

According to OPIA, motivation is a combination of one's perception of the environment, attitudes and personal needs. The doctrine of OPIA describes several factors that increase user motivation (although Spruit does not tell from which motivational theories these are derived). Below, the factors are presented together with their possible theoretical foundations (i.e. what behavioural theories they reflect, if any):

- *Reasonableness*. "People want explanations for measures that are implemented and actions they have to perform." OPIA argues that if the explanations are unsatisfactory motivation decreases. This thesis is likely to get support from the theory of cognitive moral development by Kohlberg (1981).
- *Expectancy*. The motivation depends on: the strength of the expectation that the action will be followed by a given outcome; the attractiveness of the

outcome. Such a thesis of "expectancy" may get support from the theory of reasoned action by Fishbein and Ajzen (1975), the theory of planned behaviour by Ajzen (1991) and from Vroom's (1964) expectancy theory.

- *Conformity*. "People conform their behaviour to that of other members of the group" and especially to persons who seem to hold a certain authority. This may have connections to the concept of subjective norms in the theory of reasoned action by Fishbein and Ajzen (1975) and the theory of planned behaviour by Ajzen (1991).

Thesis 3

OPIA also notes the overestimated value of the effectiveness of punishment and rewarding (we shall consider this issue in section six). OPIA divides human failing into two classes, direct and indirect failing, stating that most security breaches are not consequences of malevolent actions.

Weaknesses of thesis 3

OPIA does not provide any empirical evidence (nor references to such evidence) to support the argument about the rarity of malevolent actions. The latter reason is not a very attractive argument for ruling out the class of malevolent actions, since many people argue (e.g. Loch and Carr, 1991; Anderson, 1993; Vardi and Wiener, 1996; Neumann, 1999) that a remarkable portion of security breaches (which are malevolent by nature) are carried out by insiders.

Thesis 4

Direct failing may involve both conscious and unconscious behaviour. In the case of direct failing, one commits an error (conscious/unconscious) which leads to an interruption (and if there are no relevant security measures the security breach is more than expected) (Spruit, 1998). In Spruit's view, committing an unconscious error can be traced back to slips ("automatic actions that are wrong in the given situation") and lapses of concentration ("failures caused by flagging of concentration"). Failing in conscious behaviour, in turn, is linked to mistakes ("actions that would be correct in another situation, but not in the actual") and offences where actions are carried out (more or less) deliberately. The realm of offences consists of offences in good faith (e.g. offences that take place when the situation in question is exceptional and the rules are inapplicable; or non-exceptional cases, where there are violations of inadequate or unclear rules) and offences in bad faith.

Weaknesses of thesis 4

Another possible weakness of OPIA is closely related to the possible misinterpretation of the nature of a user-related problem. As we have seen, OPIA is emphasised in: exceptional cases; and non-exceptional ones where the rules are unclear or inadequate in terms of user-related problems (Spruit, 1998). However, even though we agree that these cases are important, the problems may also occur in normal cases, where the rules are clear. Be as it may, people often neglect most normal security procedures under normal circumstances. The simplest example of this are passwords. Although people may know, or at least they have clearly been provided with the information of what a relevant password should include and what it should exclude, we are likely to find users who still use inappropriate passwords (e.g. Morris and Thompson, 1979; Bergadano *et al.,* 1997). In this matter, the views of OPIA and the awareness community differ. While Spruit (1998) argues that things go wrong because the rules are unclear (for users), the awareness people argue further that even if they are clearly documented and distributed, users may still fail to comply with guidelines, since the rules may not be adequately reasoned. In other words, the awareness community sees that employees are not motivated seriously enough, and therefore user commitment is difficult to achieve (Spurling, 1995; McLean, 1992; Siponen, 2000a). This view (about the role of commitment) of the awareness community has been explored empirically among behavioural scientists. The result was that the level of commitment correlates to misbehaviour, so low commitment more likely implies misbehaviour (Vardi and Weiner, 1996).

Thesis 5

Indirect failing is the case when correct actions nevertheless lead to a security breach. Spruit (1998) describes the following passage as an example of such an incident (although the text has been abbreviated, the nature of the relevant events is left untouched):

> A supervisor pushes a worker to work overtime. The employee forgets to switch off his PC when he leaves the workplace. This shouldn't be a problem, however, since the guard should do this during his round, but the guard already has done his round. As a result, a cleaning person uses the possibility and copies an important piece of work and sells it to a competitor.

This type of failure, concurrence of circumstances, consists of latent failure (e.g. pressure of time and lack of arrangements for working overtime), a certain state of mind (e.g. one is tired), non-standard action (forgetting to log off), non-standard circumstances (no

security guard on his round) and disturbance (cleaning person copies a piece of classified data). According to the principles of OPIA, such negative activity can be avoided by: security measures; and identification and elimination of latent failures. It is very easy to share this view in part. According to OPIA, other activities, such as elimination of all potential non-standard actions, circumstances and the direct influence of state of mind, are not useful in preventing this kind of action from occurring.

Weaknesses of thesis 5

The first two reasons are based on arguments that are quite persuasive, while the last reason is hardly explained at all. The first argument maintains that the number of all possible non-standard actions and circumstances is simply too great to cover. Regarding the second aspect, Spruit argues that security awareness activities do not give any help with respect to the key persons in the passage. It can also be said that the key persons did not possess relevant knowledge and commitment towards the guidelines (e.g. "forgets to switch off his PC when he leaves the workplace" may be due to lack of commitment), and therefore it may make sense to increase their awareness towards a state of commitment.

Weaknesses of theses 4 and 5

As mentioned, OPIA (as well as the other approaches) leaves the state of affairs referred to as weakness of will untouched. This phenomenon refers to a situation where a person A intentionally wants to carry out X, but however (for some reason)[5] fails to do so (e.g. see Mortimore, 1971). This state of affairs, although not covered by OPIA, is more than common. Consider, for example, a person who smokes (one may be aware that one should not smoke, however in the end one still continues smoking). It is also unclear and a matter of debate whether weakness of will belongs to the category of offences in good or bad faith (following the terminology of OPIA).

Thesis 6

OPIA[6] describes "a more effective approach against human failing" (Spruit, 1998) as follows:

- Eliminate latent failures (lack of arrangements such as overtime requirements; and pressure of time, like arrangements to avoid overtime work; skills of the employees, lack of management and leadership; quality of the working environment; applicability and availability of facilities/policies/operating procedures; communication between people).
- Eliminate slips, mistakes and wanderings (the environment should be modified in such a way that the required behaviour matches the behaviour which is the most logical to one; in order to prevent unconscious failing, the aspects causing pressures or negative impulses need to be taken care of).
- Eliminate offences. In the case of exceptional situations, if the breaking of a rule is a relevant course of action, consider whether the rule needs any modification. If, in an exceptional situation, the specific rules are not clear, it has to be made known. In the case of unclear rules, OPIA does not give clear answers. Bad offences can be classified into two categories: minor offences such as "everybody does so", where the values with respect to information security need to be improved (in a wide sense, if the employees conform their behaviour to that of others); and serious offences which, following Spruit's terminology, are likely to cause serious damage to the organization – and "in such cases motivation is already totally wrong, so it is not useful to influence motivation in a subtle way". According to OPIA, it may also be useful to increase persecution measures (punishment).
- Implement additional security measures.

Weaknesses of thesis 6

The principle "eliminate offences" raises certain questions. For instance, what are the values of information security? It is difficult to see that information security per se introduces values (that are good as such) that must be respected (because they are values related to information security). Therefore, OPIA seems to put role responsibility (i.e. what is a worker's work duty set by the company) before moral responsibility (i.e. one's moral concern to do the right things). Also, OPIA seems to be able to qualify what is wrong as follows. According to Spruit (1998), if the policy of an organization is broken in such a way that it will cause serious damage to the organization, the motivation of the employees is misdirected. The heart of the problem here is that Spruit does not rule out any organizational activities. Thus, if an organization does several immoral activities, the employees not motivated towards these activities are wrong and should be punished! It has been suggested that certain actions that involve computers, considered as immoral in the final analysis, lack of relevant knowledge etc., might be partly avoided by increasing awareness of the true nature of these issues (Severson, 1997; Weckert and Adeney, 1997).

The principle "implement additional security measures" may be criticized since addition of security measures increases

operational costs (processing, maintenance, manual operations, human supervision and management), may increase the amount and likelihood of errors (since complexity increases), may restrict the normal behaviour of the systems and users, decreases the life span of IS (Baskerville, 1988), increases the duality problem (e.g. conflicting requirements between security and the systems' normal behaviour) (Baskerville, 1992) and the users of the systems may not be happy with increased security measures (may result in that security techniques and procedures are not used properly).

Finally, the principles "eliminate slips, mistakes, etc." (environment should be re-modified) and "add additional security measures" are confronted with the problem of developmental duality[7] expressed by Baskerville (1988; 1992), since OPIA does not propose any means for integrating security development and normal system development.

The organizational role of IS security, the research objective and research approach

The objectives of research of OPIA are means-oriented and interpretive. First and foremost, the main objective of OPIA is to achieve certain ends. There are also indications towards interpretive research, since the aim of OPIA is to increase people's understanding about the problems that may occur. The organizational role of IS security is socio-technical. OPIA emphasises the development of organizational systems, but equally argues for the crucial role of technical solutions. The used research method is conceptual analysis.

6. On the relevance of deterrence

Background

The concept of punishment is of ancient origin, used from the time of antiquity (Ball, 1955) to modern times. The original focus on punishment was and is socio-political. Later, the scope of punishment has extended into organizations and studies thereof have been carried out (e.g. the relevance of punishment due to violation of organizational norms/ security guidelines).

Central thesis

Economical theory of punishment holds that people avoid certain behaviour (e.g. breaking security guidelines) if they find it infeasible, frightening and so forth. In other words, the punishment works as deterrence discouraging "wrongdoing". There are other schools of punishment theories that try to justify punishment activities referring to protection of the society, reform, civil disobedience and retributivism[8] (see Warburton,1996), but they are more society-level and security researchers have not appealed to them. As the relevance of economic or "deterrence theory" rests on its consequences, so its relevance is best studied with help of empirical findings (e.g. Warburton, 1996).

The objections to use of deterrence

The critique of punishment has come from philosophers and behavioural scientists. The philosophers have considered the justness and relevance of the punishment (using conceptual analysis) mainly at the society level, while behavioural scientists have mainly explored empirically whether the punishment works (and they have also widened the consideration into the organizational level).

Although scholars of the punishment community such as Straub (1990) and Straub *et al.* (1992) have very strictly applied the criminological theories and the principles of empirical research, they have not considered the various critiques that the criminological theories have confronted. In the field of science, critique cannot be overlooked (e.g. Chalmers, 1982; Popper, 1983; 1992, p. 54), however. Since the critique against punishment, if valid, would seriously weaken the relevance of the studies by the "punishment community", it is necessary to consider it herein.

Weaknesses and open questions: long run results are negative

The results of security researchers (e.g. Parker, 1981; Straub, 1990) conflict with several studies done by the behavioural community. The security researchers suggest that punishment works well as deterrence (e.g. Parker, 1981; Straub, 1990). Although the economic theories of punishment have achieved results that support the economic theories of punishment (see e.g. Boldman and Maultby, 1997; Straub, 1990; Straub *et al.*, 1992), there is, on the other hand, much evidence of negative consequences related to the use of punishment. These "side effects" reported by behavioural scientists (e.g. Skinner, 1953; Sims, 1980; Fedor and Ferris, 1981; Podsakoff *et al.*, 1982) include loss of trust, productivity and loyalty, increased dissatisfaction and stress, aggression, fear and infeasibility (punishment does not work). For a good survey of the results, see

Appelbaum *et al.* (1998) and Sims (1980). These side effects are serious, since stress, for example, can lead to withdrawal behaviour such as turnover and absenteeism (e.g. Gupta and Beehr, 1979, pp. 373-4): "the higher the stress, the more unpleasant the work situation will be, and the more the individual will try to escape from it."

This diversity of the results may be explained by the fact that "side effects" and "long run effects" are not considered by security researchers such as Straub *et al.* (1992). Reese (1966) has postulated the fondness for the punishment by its felt capacity to immediately halt undesired activities. However, especially the long run results of the punishment activities are not considered (Podsakoff *et al.,* 1982), even though such "side effects" cannot be overlooked. As a result, we still need further empirical studies that pay attention to the mentioned "side effects" and long run consequences. Additionally, Ball (1955, p. 349) has suggested that such divergence about the relevance of punishment occurs because the effects of deterrence are individual.

The organizational role of IS security, the research objective and research approach

The view of the punishment community (Parker, 1981; Straub, 1990; Straub *et al.*, 1992) concerning the organizational role of IS security is technical. This is because the resistance (e.g. violation of security guidelines/policy) is considered as irrational, unwanted behaviour that needs to be controlled e.g. with the help of punishment. Therefore, the objective of the research is clearly means-oriented. When it comes to Straub's (1990) studies, the used research method is empirical theory testing research. Parker relies on his personal experiences.

7. Discussion

This paper analysed the various approaches to minimizing human-related faults. Of these approaches, the awareness approaches and approaches appealing to human morality were left outside the scope of the paper. The approaches were divided into two categories, namely punishment and non-punishment. The first category is described in Table III. The approaches within the first category were divided into two sections: approaches that attempt to influence different products and approaches that attempt to influence users.

Non-punishment community

As seen in Table III, there are no empirical studies in the area of the first category (the non-punishment community).

When it comes to the underlying theoretical foundations and reference disciplines, it is particularly astonishing that behavioural theories are not applied. Instead, the authors are content to: apply general textbooks (such as Spruit, 1998; Thomson and von Solms, 1998); or reflect their own experiences (Perry, 1985; Spurling, 1995). Both can be seen as weaknesses, since different behavioural theories are highly relevant and should be applied. In the same vein, scientific theories (e.g. behavioural ones), provided that they have survived scientific inspection, are in all probability more reliable than someone's personal experiences, presumptions, intuitions and speculations (e.g. Popper, 1992; Warburton, 1996; Niiniluoto, 1999). Consequently, personal experiences and speculations have no place in science (e.g. Chalmers, 1982). The most commonly used research approach was conceptual analysis. The prevailing research objective was means-oriented: all studies aimed at achieving a certain concrete goal, namely to minimize human-related faults. Spruit (1998) also has an interpretative research objective.

Within the non-punishment category, all three forms of the organizational role of IS security were found. Saltzer and Schroeder (1975) have favoured the technical organizational role of IS security. Spruit's approach emphasises the socio-technical role of IS security, while the approach by Zurko and Simon (1996) leans towards the social organizational role of IS security.

Punishment community

In the area of the second category, deterrence community (results of which are shown in Table IV), empirical studies are carried out employing criminologial theories, although Parker (1981, 1998) makes an exception by reflecting his personal experiences. The research objective of the deterrence community is means-oriented. They want to consider whether the use of punishment can be used as effective deterrence against security violations. The organizational role of IS security is socio-technical, since punishment is used in a technical sense to control the employees.

From the perspective of IS development these approaches are confronted with the problem of developmental duality (i.e. security and normal system development are carried out separately and therefore have conflicting requirements) by Baskerville

(1988; 1992). Given that approaches to minimize human-related faults propose new security requirements, they should also propose means for avoiding the duality problem.

8. Conclusions and future research issues

Several different approaches towards reducing human-related faults were explored and a new taxonomy was presented. The scope was further limited to end-user related faults. The approaches were divided into two parts: those concerned with affecting the user (e.g. OPIA, awareness) and those concerned with increasing the human-orientedness of technical solutions (or procedures), such as UCS. It should be noticed that the aim of this study was not to refute the analysed doctrines, but rather to point out some possible weaknesses in the current approaches in order to improve them.

The first category (concerned with affecting the user) has attracted more interest among scholars. However, their starting points and postulations concerning the nature of the problem are rather different. With regard to the first category (affecting the user), alas, most of the studies are not very systematic nor academically disciplined. For example, the papers may deal with behavioural issues, but still present only some of the motivational aspects on a general level or do not reflect any behavioural literature – but they rather reflect the authors' own experiences. Moreover, too often the authors are unable to put forward relevant related research and state what the real focus of their work within the area of human faults is. Also, empirical works to validate the proposal are awaited. These aspects unfortunately give an impression that the area is not adequately disciplined in the academic sense.

When it comes to the second category (punishment community), the side effects and long run results related to the use of punishment have not yet been explored.

According to our knowledge, the use of rewards has not been researched by IS security scholars. This is strange since the rewards are generally associated to human performance in a positive sense (e.g. Deci and Ryan, 1980; Podsakoff *et al.*, 1982; George, 1995). Therefore, empirical and conceptual studies in this respect are also included in the agenda for further research.

Notes

1 "I think that what is common to art, myth, science and even pseudo-science is that they all belong to something like a creative phase which allows us to see things in a new light, and seeks to explain the everyday world by reference to hidden word. ... these hypothetical words are, as in art, products of our imagination of our intuition. But in science they are controlled by criticism;

Table III
Results of the analysis of the non-punishment category

Current research	Main proposals	Research objectives	Organization role of ISS	RD	RA
Saltzer and Schroeder (1975)	Ease of safe use	Means-oriented	Technical	–	CA
Spruit (1998)	All-encompassing security guidelines are difficult to write Incident analysis Clarifying human failures Suggestions for avoiding human failures	Means-oriented Interpretive	Socio-technical	Psychology generally	CA
The products					
Zurko and Simon (1996)	Ease of use claims for security products	Means-oriented	Social	–	CA

Notes: RD refers to reference disciplines; RA denotes research approaches; and CA stands for conceptual analysis

Table IV
The results of the analysis of the deterrence community

Category 2: Punishment/ deterrence community	Straub (1990) Straub *et al.* (1992)	Punishment as deterrence is relevant	Means-oriented	Technical	Criminology	Empirical: survey
	Parker (1981, 1998)	Punishment as deterrence is relevant	Means-oriented	Socio-technical	–	–

scientific criticism, rational criticism, is guided by the regulative idea of truth. We can never justify our scientific theories, for we can never know whether they will not turn out to be false. But we can subject them to critical examination: rational criticism replaces justification. Criticism curbs the imagination, but does not put it in chains. So science is characterized by rational criticism which is guided by the idea of truth, whereas the imagination is common to all creative activity, be it art, myth or science" (Popper, 1992, p. 54).

2 The existence of such a vacuum is commonly agreed on by computer ethicists, e.g. because people are unaware of technical or factual issues related to the use of computer technology (Severson, 1997).

3 Most of the work in this area has been carried out by the CHI community and not in the area of information security (Zurko and Simon, 1996).

4 They also state that mathematical rigorousness was emphasised over usability.

5 This reason rules out mistakes in the sense described by OPIA.

6 OPIA provides the following list of such functions: the work must be challenging, it should provide enough variation and there should be possibilities for relaxation.

7 Refers to a situation where IS development and security development are done separately resulting e.g. in conflicts between security and other behaviour/normal development of the system (Baskerville, 1992).

8 Retributivism holds that wrongdoers should be punished irrespective of whether the punishment helps or not (thus, it is a deontological view since the consequences do not matter).

References and further reading

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

Anderson, T.E. (1993), "Management guidelines for PC security", *Proceedings of the 1992 ACM/SIGAPP Symposium on Applied Computing (Vol. II): Technological Challenges of the 1990s*, Kansas City, KS.

Angel, I. (1993), "Computer security in these uncertain times: the need for a new approach", *Proceedings of the 10th International Conference on Computer Security, Audit and Control (CompSec)*, London, October.

Appelbaum, S.H., Bregman, M. and Moroz, P. (1998), "Fear as a strategy: effects and impact within the organization", *Journal of European Industrial Training*, Vol. 22 No 2, pp. 113-27.

Ball, J.C. (1955), "The deterrence concept in criminology and law", *The Journal of Criminal Law, Criminology and Police Science*, Vol. 46, pp. 347-54.

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

Baskerville, R. (1988), *Designing Information Systems Security*, John Wiley Information Systems Series, New York, NY.

Baskerville, R. (1992), "The developmental duality of information systems security", *Journal of Management Systems*, Vol. 4 No. 1, pp. 1-12.

Bergadano, F., Crispo, B. and Ruffo, C. (1997), "Proactive password checking with decision trees", *Proceedings of the 4th ACM Conference on Computer and Communication Security*, Zurich.

Bernstein, D.A., Clarke-Stewart, A., Roy, E.J., Sprull, T.K. and Wickens, C.D. (1994), *Psychology*, Houghton Mifflin Company, Boston, MA.

Bishop, M., Cheung, S. and Wee, C. (1997), "The threat from the net [Internet security]", *IEEE Spectrum*, Vol. 34 No 8.

Boldman, P.M. and Maultby, C. (1997), "Crime, punishment and deterrence in Australia: a further empirical investigation", *Journal of Social Economics*, Vol. 24, pp. 884-901.

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

Chalmers, A.F. (1982), *What Is This Thing Called Science?*, 2nd ed., Open University Press, Buckingham.

Chua, W.F. (1986), "Radical developments in accounting thought", *Accounting Review*, Vol. 61 No. 5, pp. 583-98.

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. (1980), "The empirical exploration of intrinsic motivational processes", in Berkowitz, L. (Ed.), *Advances in Experimental Social Psychology*, Academic Press, Vol. 13, pp. 39-80,

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

Fedor, D.B. and Ferris, G.R. (1981), "Integrating OB MOD with cognitive approaches to motivation", *Academy of Management Review*, Vol. 6 No. 1, pp. 115-25.

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

George, J.M. (1995), "Asymmetrical effects of rewards and punishment: the case of social loafing", *Journal of Occupational & Organizational Psychology*, Vol. 68 No. 4, pp. 327-440.

Gupta, N. and Beehr, T.A. (1979), "Job stress and employee behaviours", *Organizational Behaviour & Human Performance*, Vol. 23 No. 3, pp. 373-87.

Information Management & Computer Security
8/5 [2000] 197–209

Harrington, S.J. (1996), "The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions", *MIS Quarterly*, Vol. 20 No. 3, September.

Iivari, J. (1991), "A paradigmatic analysis of contemporary schools of IS development", *European Journal of Information Systems*, Vol. 1 No. 4, pp. 249-72.

Iivari, J. and Hirschheim, R. (1996), "Analyzing information systems development: a comparison and analysis of eight IS development approaches", *Information Systems*, Vol. 21 No. 7, pp. 551-75.

Iivari, J. and Kerola, P. (1983), "A sociocybernetic framework for the feature analysis of information systems design methodologies", in Olle, T.W., Sol, H.G. and Tully, C.J. (Eds), *Information Systems Design Methodologies: A Feature Analysis*, North-Holland, Amsterdam, pp. 87-139.

Iivari, J., Hirschheim, R. and Klein, H. K., (1998), "A paradigmatic analysis of contrasting information systems development approaches and methodologies", *Information Systems Research*, Vol. 9 No. 2, pp. 164-93.

Järvinen, P. (1997), "The new classification of research approaches", in Zemanek, H. (Ed.), *The IFIP Pink Summary – 36 Years of IFIP*, IFIP, Laxenburg.

Järvinen, P. (2000), "Research questions guiding selection of an appropriate research method", *Proceedings of the 8th European Conference on Information Systems (ECIS 2000)*, 3-5 July, Vienna.

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

Kowalski, S. (1990), "Computer ethics and computer abuse: a longitudinal study of Swedish university students", *IFIP TC11 6th International Conference on Information Systems Security*.

Kukathas, C. and Pettit, P. (1990), *Rawls – A Theory of Justice and its Critics*, Stanford University Press, Stanford, CA.

Leiwo, J. and Heikkuri, S. (1998a), "An analysis of ethics as foundation of information security in distributed systems", *Proceedings of the 31st Hawaiian International Conference on System Sciences (HICSS-31)*, Hawaii, January.

Leiwo, J. and Heikkuri, S. (1998b), "A group-enhanced ISSI model for secure interconnection of information systems", *Proceedings of the IFIP TC11, 14th International Conference on Information Systems Security (IFIP/Sec'98)*, Vienna, and Budapest.

Loch, K.D. and Carr, H.H. (1991), "Threats to information system security: an organizational perspective", in *Proceedings of the Twenty-Fourth Annual Hawaii International Conference on System Sciences (HICSS)*.

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

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 Systems Research*, Vol. 3 No. 2, pp. 173-91.

Morris, R. and Thompson, K. (1979), "Password security: a case history", *Communication of the ACM*, Vol. 22 No. 11, pp. 594-7.

Mortimore, G. (Ed.) (1971), *Weakness of Will*, Macmillan, London.

Neumann, P.G. (1999), "Inside risks: risks of insiders", *Communication of the ACM*, Vol. 42 Issue 12, p. 160.

Niiniluoto, I. (1990), "Science and epistemic values", *Science Studies*, Vol. 3 No. 1, pp. 21-5.

Niiniluoto, I. (1999), *Critical Scientific Realism*, Oxford University Press, Oxford.

NIST (1995), *The NIST Handbook*, (1995), *An Introduction to Computer Security*, NIST special publications, 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. (1981), *Computer Security Management*, Prentice-Hall, Englewood Cliffs, NJ.

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

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

Podsakoff, P.M., Todor, W.D. and Skov, R. (1982), "Effects of leader contingent and noncontingent rewards and punishment behaviours on subordinate performance and satisfaction", *Academy of Management Journal*, Vol. 25 No. 4, pp. 810-21.

Popper, K.R. (1983), *The Logic of Scientific Discovery*, 11th ed., Hutchinson, London.

Popper, K.R. (1992), *In Search of a Better World: Lectures and Essays from Thirty Years*, Routledge, London.

Reese, E.P. (1966), *The Analysis of Human Operant Behavior*, William C. Brown, Dubuque, IO.

Robbins, S.P. (1998), *Essentials of Organizational Behaviour*, Prentice-Hall, Englewood Cliffs, NJ.

Saltzer, J.H. and Schroeder, M.D. (1975), "The protection of information in computer systems", *Proceedings of the IEEE*, Vol. 63 No. 1, September.

Sandhu, R. and Jajodia, S. (1995), "Integrity mechanism in database management systems", in Abrams, M.D., Jajodia, S. and Podell, H.J. (Eds), *Information Security – An Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamitos, CA.

Severson, R.J. (1997), *The Principles of Information Ethics*, M.E. Sharpe, Armonk, NY.

Sims, H.P. (1980), "Further thoughts on punishment in organizations", *Academy of Management Review*, Vol. 5 No. 1, pp. 133-8.

Siponen, M.T. (1999), "Analysis of different approaches to cope with user related faults in IT security", *Proceedings of 11th Annual Canadian Information Security Symposium*, 10-14 May, Ottawa.

Siponen, M.T. (2000a), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 Issue 1.

Siponen, M.T. (2000b), "On the role of human morality in information system security: the problems of descriptivism and non-descriptive foundations", *15th International Information Security Conference (IFIP TC11/ SEC2000)*, Beijing.

Siponen, M.T. (2000c), "An analysis of the recent IS security development approaches: descriptive and prescriptive implications", in Dhillon, G. (Ed.), *Information Security Management – Global Challenges in the Next Millennium*, Idea Group.

Skinner, B.F. (1953), *Science and Human Behaviour*, Macmillan, New York, NY.

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", SEC, TC11, Vienna.

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

Straub, D., Carson, P. and Jones, E. (1992), "Deterring highly motivated computer abuses: a field experiment in computer security", in Gable, G.G. and Caelli, W.J. (Eds), *IT Security: The Need for International Cooperation*, North Holland, Amsterdam, pp. 309-24.

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

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.

Straub, D.W. and Widom, C.P. (1984), Deviancy by bits and bytes", in Finch, J.H. and Dougall, E.G. (Eds), *Computer Security: A Global Challenge*, Elsevier Science Publisher, Barking.

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.

Warburton, N. (1996), *Philosophy: the Basics*, 2nd ed., T.J. Press, Padstow, Cornwall.

Weckert, J. and Adeney, D. (1997), *Computer and Information Ethics*, Greenwood Press. Westport, CT.

Vardi, Y. and Wiener, Y. (1996), "Misbehavior in organizations: a motivational framework", *Organization Science*, Vol. 7 No. 2, March-April, pp. 151-65.

Vroom, V.H. (1964), *Work and Motivation*, John Wiley & Sons, New York, NY.

Zurko, M.E. and Simon, R.T. (1996), "User-Centered Security", ACM New Security *Paradigms Workshop,* 17-20 September, Lake Arrowhead, CA.