Journal of the Association for Information Systems

Volume 7 | Issue 7 Article 19

7-28-2006

Six Design Theories for IS Security Policies and Guidelines

Mikko Siponen
University of Oulu, Finland, mikko.t.siponen@jyu.fi

Recommended Citation
Siponen, Mikko (2006) "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems*, 7(7), .
DOI: 10.17705/1jais.00095
Available at: https://aisel.aisnet.org/jais/vol7/iss7/19

Journal of the Association for Information Systems

Research Article

Six Design Theories for IS Security Policies and Guidelines [1]

Mikko Siponen
Department of Information Processing Science
University of Oulu, Finland
mikko.siponen@oulu.fi

Juhani Iivari
Department of Information Processing Science
University of Oulu, Finland
Juhani.iivari@oulu.fi

Abstract

The unpredictability of the business environment drives organizations to make rapid business decisions with little preparation. Exploiting sudden business opportunities may require a temporary violation of predefined information systems (IS) security policies. Existing research on IS security policies pays little attention to how such exceptional situations should be handled. We argue that normative theories from philosophy offer insights on how such situations can be resolved. Accordingly, this paper advances six design theories (the conservative-deontological, liberal-intuitive, prima-facie, virtue, utilitarian and universalizability theories) and outlines the use of their distinctive application principles in guiding the application of IS security policies. Based on the testable design product hypotheses of the six design theories, we derive a theoretical model to explain the influence of the different normative theories on the "success" of IS security policies and guidelines.

Introduction

The functioning of modern society is increasingly reliant on computers and global networks. In such a society, information systems security, aimed at ensuring the confidentiality, integrity, and availability of information, becomes a very important issue. Not only do security violations cause loss of valuable information and damage the organization's reputation, but they also prevent organizations from trading. Hence, it is

[1] Kalle Lyytinen was the accepting senior editor. Sirkka Jarvenpaa and Yair Wand were the reviewers. The earlier version of this paper was presented in the JAIS theory workshop at ICIS 2004. It was submitted on March 15, 2005, and went through 3 revisions.

important to ensure that organizations' ISs are properly secured. While a number of technical solutions and secure system development methods exist for securing organizations' systems (Backhouse and Dhillon, 2001; Siponen, 2005), both practitioners and scholars agree that an IS security policy, and its enforcement, is the necessary foundation of organizations' IS security (e.g., Parker, 1997; Straub, 1990; Warman, 1992). In organizations whose future circumstances are difficult to predict in advance (Boyd and Fulk, 1996 p. 4; Daft, et al., 1988 p. 125), unexpected business opportunities may require actions that conflict with their IS security policy. In such situations, word-for-word compliance with a rigid IS policy may prevent organizations from taking advantage of such unanticipated business opportunities. We refer to these as exceptional situations.[2]

While such exceptional situations are recognized in IS security literature (Baskerville, 1995 p. 245; Dhillon and Backhouse, 2000 p. 126), extant research does not address how these exceptional situations should be handled.

In trying to understand under what conditions normative IS security policies and guidelines may be violated, we find normative theories in philosophy extremely useful. Accordingly, this paper presents six design theories in the sense of Walls, Wildmeyer and El Sawy (1992) for the application of IS security guidelines in exceptional situations, influenced by normative theories in philosophy. Based on the testable design product hypotheses of the six design theories, we derive a theoretical model to explain the influence of the different normative theories on the "success" of IS security policies and guidelines.

Research into IS security policies and guidelines in exceptional situations has value for scholars and practitioners. For scholars, the paper advances a foundation for future research on how to balance IS security and business opportunities in exceptional situations. For practitioners, the paper offers insights on how they may apply wisdom from applied philosophy in solving exceptional situations in practice.

This paper is organized in six sections as follows. In the Section "Design Theories and Existing Work on Security Policies",, an IS security policy design theory framework is first elaborated, including the three criteria for IS security polices and guidelines. Then, existing studies on IS security policies are scrutinized in order to point out the extent to which the extant studies on IS security policies meet these three criteria. At the end of the Section, it is pointed out that extant works on IS security policies do not address the third criterion (how to apply IS security guidelines and policies in exceptional situations). The Section "Philosophical Normative Theories and IS Security Policies and Guidelines" outlines normative theories for IS policies and guidelines, introducing six normative theories as kernel theories for IS security policies and guidelines, and Section "The Six Normative Theories and Design Theories for IS Security Policies and Guidelines" discusses these in more detail. Then an agenda for future research on the application of IS security policies and guidelines is proposed in the "Discussion" section. In the final section, the key findings of the paper are summarized.

[2] Note that conceptually these 'exceptional situations' differ from 'exceptions' as "cases that cannot be correctly be processed by computer systems alone" (Strong and Miller, 1995, pp. 206). While the exceptional situations may be addressed following the organization's IS security policies and guidelines, this may not be reasonable from the viewpoint of their business objectives.

Design Theories and Existing Work on Security Policies

IS Design Theorizing and Security Policies

Walls, Wildmeyer and El Sawy (1992) propose that design theories should be based on kernel theories and should inform the researcher by providing testable research hypotheses. They see IS design theories as having two dimensions: a product (e.g., a software product or security policy) and a design process (the phases to be followed in constructing the product) – see Figure 1. In addition, design theories are normative and prescriptive, as opposed to theories in natural science, which are descriptive, explanatory, and predictive (Markus, *et al*., 2002; Walls, *et al*., 1992 p. 37).

Hevner, March, Park and Ram (2004 p. 77-78) recognize that designing policies is a potential application of design theory. In this paper, we view IS security policies and guidelines as design products. Typically, IS security policies and guidelines are normative lists of actions that the employees should (or should not) perform (Warman, 1992 p. 309). However, the design of IS security policies and guidelines faces the problem that such policies and guidelines do not necessarily make it possible to address all situations reasonably. To illustrate this, Puhakainen (2006) describes a company in which IS security guidelines strictly forbid taking any information away from the company

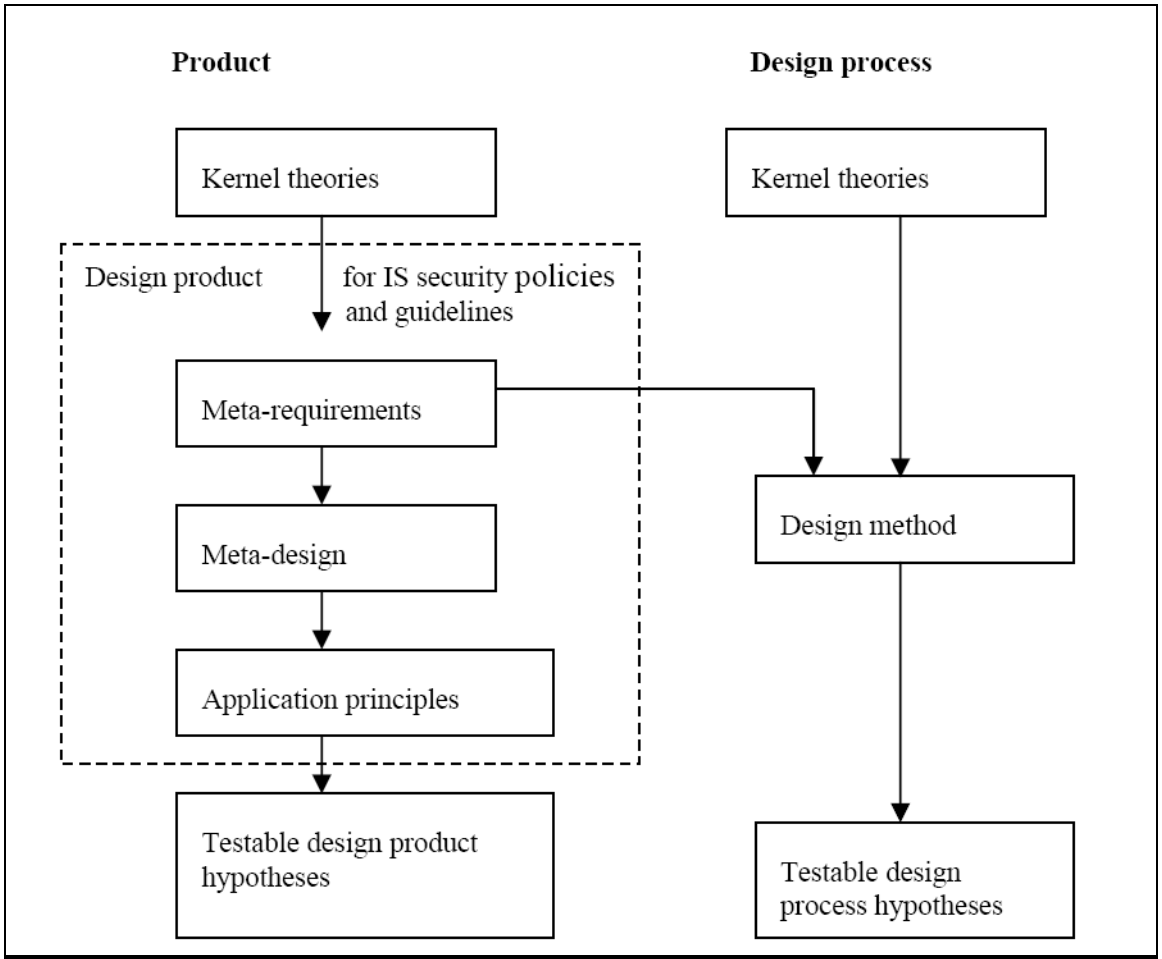

Figure 1. An IS security policy design theory (modified from Walls, *et al*., 1992)

premises without formal permission from the IS security manager. However, the employees of the company needed to take their laptops, USB sticks, and CDs to their homes and to meetings outside of the company. As a result, employees violated the IS security policy, since in some cases they felt they would lose their customers and collaborators if they waited for the formal approval process.

The product is the IS security policy or guideline, also including an application principle stating how the IS security policies and guidelines are to be applied. The design method states how the product (IS security guideline) is to be crafted. Application principles may also guide the design of IS security policies and guidelines.

As this case illustrates, it is important to know whether the policies and guidelines can be violated by employees in a situation where word-for-word compliance with them would jeopardize a business opportunity. And if they can, under what conditions and in what circumstances is this permissible? We claim that IS security policies and guidelines should be equipped with 'application principles' to solve such exceptional situations (Figure 1). Recognizing this, a design theory for IS security policies should meet three criteria – it should: (1) be based on kernel theories; (2) offer normative guidance for practitioners on how to design and apply such policies and guidelines;[3] and (3) propose a research agenda (testable hypotheses) for scholars (Walls, *et al*., 1992).

Extant Security Policies in the Light of IS Security Policy Design Theory

This section examines the extent to which existing approaches to IS security policy address these three IS security design theory criteria (Table 1).

Criterion 1: Kernel theories

The underlying kernel theory provides the necessary foundation on which guidance for practitioners and a research agenda can be developed (Markus, *et al*., 2002). Of the extant studies, only Karyda, Kokolakis and Kiountouzis (2003) is explicitly derived from a reference discipline (first criterion). The lack of theoretical underpinnings may explain why studies on IS policies fail to offer concrete guidance to practitioners as to how to design IS security policies and how possible exceptional situations can be handled (criterion 2).

Criterion 2: Application principles

The application principles should provide advice on how to handle exceptional situations (second criterion), since adherence to a security policy in certain circumstances may prevent the achievement of business objectives (for example, a business opportunity suddenly emerges, but cannot be taken advantage of, as it would violate IS security policy and guidelines).

Existing IS security policies do not provide advice on how to handle exceptional situations (criterion 4). Even though Corby (1999), Hale (1996), Palmer, Robinson, Patilla, and Moser (2001 p. 22), and Wood (1997c p. 16) recognize the need to make exceptions, of all the existing IS security policy studies, only Dhillon and Backhouse (2000)

[3] Application principles are not covered by the original design theory framework of Walls, Wildmeyer and El Sawy (1992).

Table 1. Existing IS Security Policy Approaches and the Three IS Security Design Theory Criteria [4]

Approach	Criterion 1: Kernel theories	Criterion 2: Application principles	Criterion 3: Testable hypotheses
Baskerville and Siponen (2002)	?	-	?
Broderick (2001)	-	-	-
BS7799	-	-	-
Corby (1999)	-	-	?
Dhillon (1997)	-	-	-
Dhillon and Backhouse (2000)	-	?	-
David (2002)	-	-	-
Friedl (1990)	-	-	-
Fulford and Doherty (2003)	-	-	+
Hale (1996)	-	-	-
Hickson (1997)	-	-	-
Höne and Eloff (2002)	-	-	-
ISF Standard (2003)	-	-	-
Karyda *et al*. (2002)	+	-	?
Lindup (1995)	-	-	-
Nosworthy (2000)	-	-	-
Olnes (1994)	-	-	-
Osborne (1998)	-	-	+
Palmer *et al*. (2001)	-	-	-
Pounder (1997)	-	-	-
Pounder (2001)	-	-	-
Pounder (2002)	-	-	-
SSE-CMM (1998)	-	-	-
Walter (1993)	-	-	-
Warman (1992)	-	-	?
Wood (1995)	-	-	-
Wood (1996a)	-	-	-
Wood (1996b)	-	-	-
Wood (1996c)	-	-	-
Wood (1997a)	-	-	-
Wood (1997b)	-	-	-
Wood (1997c)	-	-	-
Wylder (2003)	-	-	?

can be regarded as providing guidance on how to handle exceptional situations (criterion 2: application principles). Dhillon and Backhouse (2000 p. 127-128) propose four principles: responsibility, integrity, trust, and ethicality. Although their work makes a novel contribution, it is not quite clear how their principles can be applied in practice (how does one know what an "ethical" action is, for example?), or how to proceed if these principles are in conflict with the business objectives of the company.

[4] The symbol + means that the approach meets the criterion, and – refers to a lack of such a feature. The symbol ? means that, even though the approach does not explicitly address a certain criterion, there are implicit hints as to the existence of such a feature.

Criterion 3: Testable hypotheses

'Testable hypotheses' refers to systematic research agendas that guide future research on IS security policies. While the approaches of Corby (1999), David (2002), Fulford and Doherty (2003), Karyda, Kokolakis and Kiountouzis. (2003), Osborne (1998), Baskerville and Siponen (2002), Warman (1992), and Wylder (2003) may be interpreted as having testable hypotheses or a research agenda (criterion 3), none of these studies present testable hypotheses with regard to application principles (criterion 2).

Summarizing the analysis of 33 IS security policy studies, a few approaches address one or two of the IS security design theory criteria: kernel theories (criterion 1) and testable hypotheses (criterion 3), but none of them address guidelines to cover exceptional cases (criterion 2). Therefore, there is a need to seek alternative normative theories to guide application of IS security policies and guidelines.

Philosophical Normative Theories and IS Security Policies and Guidelines

Introduction

In seeking candidate kernel theories, we found the normative theories to constitute ideal reference theories for the application principles, for two reasons. First, IS design-oriented theories are normative and prescriptive, in contrast to natural science theories, which are explanatory or predictive (Walls, *et al*., 1992). IS security policies are also seen as mandatory by nature (Wood, 1995): they lay down the IS security actions (the list of "dos and don'ts") that employees should follow in general. Second, an IS security policy design theory should contain normative application principles on how to apply the list of 'dos and don'ts' (the security policies and guidelines) in exceptional situations.

Recognizing this normative dimension, there is no doubt about what constitutes the ideal theoretical foundation (or kernel theory base) for the application principles: normative theories in philosophy. While empirical social sciences investigate what people do, normative theories ponder what people should do (Hare, 1997).[5] Indeed, in the domain of normative theories, from Aristotle through Kant, and up to present-day thinkers, scholars have sought answers to such questions as how to a settle a conflict between two different norms, or how to act in cases where conforming to the established norm yields negative results. These problems are similar to those studied in this paper. Finally, the history of normative theories is more than 2,500 years old; thus, normative theories are mature in comparison to any other discipline. This being the case, normative theories are ideal candidates for kernel theories in the context of the present study.

Alternative normative theories include the theory of information ethics (Floridi, 1999), Habermas' (1990) discourse ethics, universal prescriptivism (Hare, 1952, 1963, 1981, 1999), Kantian ethics (Kant, 1993), utilitarianism (e.g., Bentham, 1876; Mill, 1895), intuitionism (Ross, 1930), Mackie's (1981) approach, the theory of justice (Rawls, 1972), emotivism (Stevenson, 1944), and virtue ethics (e.g., Hursthouse, 1996; MacIntyre, 1987).

[5] Hume (1711-1776) warns us, in his thesis of "no ought from an is", about the logical problem of basing a normative action on empirical knowledge alone.

Six Normative Theories for IS Security Policies and Guidelines

Of these alternative normative theories, we have selected six main categories of theories to form the basis for alternative application principles. These are the conservative deontological, the liberal-intuitive, the *prima-facie*, the virtue ethics, the utilitarian, and the universalizability theories. We do not claim that these six theories form the only way of categorizing normative theories. They do, however, cover a large body of extant normative theories, and they have obvious applicability for IS security policies and guidelines, as will be illustrated below (Table 2).

Table 2. Alternative Normative Theories on Which to Base Application Principles

Normative theories	Recognize exceptional situations	Method for handling the exceptional situations
The conservative deontological	No	No method is provided
The liberal-intuitive	Yes, but does not take any normative stance	No method is provided
Prima-facie	Yes	Benefit
The virtue ethics	Yes	Virtues
The utilitarian	Yes	Overall happiness
The universalizability theories	Yes	Universality thesis

Deontological theories hold that objective moral rules exist. The *conservative deontological theory* stems from deontological moral norms, such as Kant's doctrine of treating humans as an end rather than as a means (Kant, 1993). Another form of conservative deontological theory is present in Judeo-Christian teachings, where the Ten Commandments are interpreted literally. So, according to conservative deontological theory, rules in normative systems are absolute, predefined and intended to be followed literally. When applied to IS security policies and guidelines, rules in conservative deontological IS security policies and guidelines must be followed to the letter without thinking about possible consequences.[6] And, if some situation is not explicitly addressed in the conservative deontological IS security guideline, e.g., taking information off company premises (cf., example in section 2.1), then the action is not allowed by default.

The opposite view to the conservative deontological theory is the *liberal-intuitive theory*, stemming from libertarianism. It holds that if something is not forbidden, it is allowed. In the case of IS security policies and guidelines, this means that if certain IS security situations are not covered by the IS security polices and guidelines, then employees are allowed to do whatever they want to in those situations[7], [8]. While the conservative deontological theory does not recognize exceptional situations at all (since if something is not addressed in the IS security policy, it is forbidden), the liberal-intuitive theory does not give any methodological advice on how to act in exceptional situations. To counter

[6] Lupu and Sloman (1999 p. 854) call this policy the "negative authorization policy".
[7] It stresses minimal external regulation and the maximization of the autonomy of the individual over authority: "Liberty can be restricted only for the sake of liberty" (Kukathas and Pettit, 1990 p. 50).
[8] Lupu and Sloman (1999 p. 863) refer to a similar policy as the "open policy"; otherwise we find no examples on the liberal-intuitive theory in IS security literature.

this problem, a number of alternative theories (the *prima-facie*, the virtue ethics, the utilitarian, and the universalizability theories) have been advanced.

The *prima-facie* theory from Ross (1930) recognizes exceptional situations. Applied to IS security, it takes the view that security guidelines should be followed in general. In exceptional situations, however, one may violate them if the business benefits of compromising the guidelines outweigh the benefits of complying with them.
While the prima-facie theory focuses on calculating benefits, virtue ethics, forming the *virtue design theory* (Hursthouse, 1996; MacIntyre, 1987), suggest that we should instead develop virtues personally. Virtues are praiseworthy qualities or characteristics that people may possess.[9] MacIntyre extracts unitary core concepts for the virtue design theory from different theories of virtue ethics: the virtues of justice, courage, and honesty (MacIntyre, 1987 p. 123 and 128).[10] Virtue ethics (MacIntyre, 1987) and Christian theology[11] also adhere to the thesis of supererogation. In philosophy, supererogation refers to positive actions that go beyond what is required. Supererogatory actions are praiseworthy, yet at the same time voluntary. For example, an elderly or disabled person putting his or her life at very high risk in an attempt to save others from a fire may be considered a supererogatory action. The person acted virtuously, but had the person not taken the action, he could not be regarded as blameworthy. Applied to IS security policies and guidelines, the idea of supererogation means that the IS security policy and guidelines prescribe an ideal or a virtuous code of conduct for the organization's employees to follow. Thus, actions in conflict with the IS security policies and guidelines are not deemed to be wrong or punishable.

While the *prima-facie* theory stresses the business benefits and the *virtue theory* stresses cultivation of proper virtues in exceptional situations, the *utilitarian theory* (Bentham, 1876; Mill, 1895) suggests that the key issue is the maximization of utility. According to Bentham, the key idea in maximizing utility is the concept of felicity (happiness). For Bentham, felicity is a combination of pleasure and the absence of pain.[12] Thus, in a nutshell, utilitarianism holds that an act that produces the greatest felicity for the greatest number of people, measured in terms of pleasure and absence of pain, is the right action.

The *universalizability theory*, in turn, suggests that rather than relying on relativistic virtues and calculating benefits (*prima-facie*) or overall happiness (utilitarianism), an acceptable action should be one that the person would also accept if he were on the receiving end of the action. According to another interpretation, we should only accept those actions that we could accept no matter what position we held in society or the

[9] MacIntyre divides the theories of virtue ethics into three categories: (1) virtues enable individuals to perform well in their social roles (e.g., a judge in court is a social role and it can be seen that judge is expected to be impartial and just; hence the virtues of a judge may include impartiality and justness); (2) virtues enable us to move towards the achievement of a certain ultimate natural or supernatural purpose (human telos) (as suggested by Aristotle, the New Testament, and Aquinas); (3) virtues contribute to the achievement of heavenly and earthly success (as suggested by Franklin) (MacIntyre, 1987 p. 122).
[10] MacIntyre does, however, leave the door open for other possible virtues.
[11] In theology, supererogation refers to good acts done in "a state of grace".
[12] Other forms of utilitarianism include negative utilitarianism, which is aimed at maximizing the absence of pain.

organization.[13] Variations of the universality theses form the foundations of Kantian ethics, universal prescriptivism (Hare, 1981), the theory of justice (Rawls, 1971), and Judeo-Christian ethics.

A Case to Illustrate the Six Normative Theories

In this real case, a project team in a software house maintains close collaboration with customers when developing software. This software house has strict security rules laid down by a senior security specialist, who is regarded as the authority figure. The security policy includes a rule that states that passwords are personal and that one's password cannot be given to anybody else. Any exception must be approved by the senior security specialist. During the summer, while the senior security specialist and most of the developers are on their holidays, a few members of the project team receive additional requirements and feature changes from an important customer. The members of the team need to make changes to the software quickly to keep to their deadline. To do this they need to access some files to which they currently do not have access (access can be granted by a developer and the security specialist or his subordinates). The senior security specialist cannot be reached at that time, and the developer who has control over the files is also on holiday. He is available, but cannot remember his password (he forgot it while on holiday). Subordinates of the senior security specialist can be contacted, but they do not dare to violate the IS security policy of the organization. As a result, the members of the project team are forced to wait for the senior security specialist to return in order to access the files. This will result in the software company missing the deadline.

According to the conservative-deontological theory, the IS security policy cannot be violated, and therefore, in the above case, the subordinates of the senior security specialist should not violate the security policy of the organization under any circumstances. The subordinates must obey the security rules in all circumstances, and according to these rules the security specialist's approval must be awaited. In this case, the liberal-intuitive theory desires the same response, since according to the security rules of the organization, every exception must be approved by the senior security specialist.

According to the *prima-facie* theory, IS security policy can be violated provided that (i) business objectives and security requirements are in conflict, and (ii) the benefits of compromising those guidelines outweigh the benefits of complying with them. In this situation, the subordinates realize that the first condition is met. On the one hand, security rules dictate that the subordinates cannot grant access for the other members of the team. On the other, if access is not granted, negative ramifications for business may result, including losing an important client. Thus, in light of the *prima-facie* theory, given that the violation of the IS security policy would maximize business benefits, the IS security policy can be violated.

[13] According to Rawls (1971), the universalizability thesis makes us ask what principles of justice we would choose to govern a society or an organization in which, as members of it, we could be anyone in any position (Rawls, 1971). Or, according to another interpretation of thesis: "…we accept only those moral prescriptions which we are prepared to prescribe for all similar cases, no matter what position we ourselves occupy in them." (Hare, 1996 p. 177).

The virtue theory regards IS security policy compliance as voluntary, Thus, while adherence to the IS security policy is regarded as positive (as a 'virtue'), the subordinates of the senior security specialist can exercise their own judgment if they wish. Moreover, according to virtue ethics, in exceptional situations the employees' own judgment is acceptable if the actions are regarded as just, honest, and courageous. Which actions are just, honest, and courageous depends on the organizational culture in question. The subordinates may believe that in this scenario, for instance, just and honest imply that the action should be carried out in the firm's and their customer's best interests, without violating anyone's rights. Recognizing that the subordinates can use their own judgment, and provided that violating the security rules in this case can be seen as just and honest as discussed above, the subordinates may violate the security rules and grant access to these project team members.

If the software house had a utilitarian theory in place, they would need to follow the IS security guidelines in normal circumstances. In exceptional situations, or situations suspected to be exceptional, a resolution is arrived at by means of utilitarian happiness calculus. The subordinates of the security manager realize that this is not a normal situation. In order to implement the suddenly-emerged requirement from the important customer during the holiday season, the team members need to access certain files. To decide whether they can bypass the security rules, the subordinates should, according to the utilitarian theory, calculate the happiness of the greatest number of people, taking into account the absence of pain, and should favor the option that maximizes the overall happiness. Here "people" would refer to those persons affected by the decision on whether or not to violate the security rules. On the one hand, the security specialist's subordinates may consider that a violation of the security policy will probably anger the security specialist. Thus, in utilitarian terms, non-compliance with the security rules causes unhappiness to the security manager. On the other hand, given the urgent business need to meet the requirements of the important customer, the violation of the IS security policy would in this case maximize the overall happiness in the company because complying with the IS security policy and guidelines results in the developers not being able to keep to the deadline. This is assumed to have two types of negative implications. First, they may lose the important customer, which may have direct monetary consequences. Second, it is assumed that maintaining tight security rules for their own sake in this case may cause dissatisfaction (unhappiness) among the team members, as they would feel that they were not able to do their work. Recognizing these factors, while disobedience to the security rules may increase the security manager's unhappiness, the important customer's and team members' feelings of unhappiness that would result from non-compliance are much greater. Hence, if the subordinates are following utilitarian IS security policy theory, they should compromise the security rules in this situation.

In the case of the universalizability theory, the IS security policy can be violated in exceptional situations, provided that the action in question satisfies one of the two universalizability rules. Let us assume that the company has adopted the second rule of the universalizability theory: if you were the president of the organization, would you allow action Y by any trustworthy X? Here, Y refers to violation of the IS security policy in order to speed up software development, and X refers to the members of the project group who need access to the files. In this case, the senior security specialist's subordinates ponder whether they would allow the action if they were in the company president's shoes. Recognizing the business need to violate the security policy, the security specialist's subordinates see no reason why the president of the company

would not allow a violation of the security rule in this case. Adherence to the IS security policy would mean that the software would not be developed as agreed with the client, which would result in financial loss for this project (and perhaps also in the future, through loss of contracts), a bad reputation, and so on. Thus, in the light of the universalizability theory, the subordinates can violate the IS security policy.

The Six Normative Theories and Design Theories for IS Security Policies and Guidelines

Next we will describe the six normative theories as potential bases for design theories for IS security policies and guidelines. While it is impossible to list all exceptional situations in different companies,[14] the application principles can be used to scrutinize whether IS security policies and guidelines can be violated in any given situation. The reader may then wonder why we need IS security policies or other norms. Instead, why not just use application principles in all situations? There is a practical reason for this. We may not have time to ponder all the situations we face every day by using the application principles. For all these "ordinary situations" we encounter, the established norms, like IS security policies and guidelines, are useful (cf., Hare, 1981; Twining and Myers, 1999 p. 15).

Furthermore, normative theories in socio-politics and ethics typically ponder what is morally right for individuals. In this paper, we have made a point of departure by focusing on what is in the company's interest. Our application of the normative theories is business-oriented: how can they be applied in the design of IS security policies and guidelines and application principles so that the IS security policies, guidelines, and application principles as a whole will serve the company in the best way? For this purpose, we will introduce the concept of Total Cost of Security Actions (TCSA). TCSA functions as the dependent variable to be minimized. TCSA is a measure of all costs resulting from developing IS security polices and guidelines, from violating them, and from complying with them. Thus, TCSA covers all costs that can be attributed to an IS security violation, including immediate recovery costs and potential losses, such as lost business opportunities or loss of reputation for the business. TCSA also includes the costs of potential loss of business opportunities resulting from adherence to the IS security policies and guidelines. For example, in the case presented in section 3.3, strict adherence to the IS security policies and guidelines results in the developers being unable to deliver the software to the client in time. This may damage their reputation in the eyes of the important client and lead to sanctions for not keeping the deadline. These, in turn, increase the risk that the important client will order its future software from competitors. Since such costs are different in different organizations and situations, it is impossible to provide a more explicit list of cost factors.

Our analysis follows the structure of the design product side of Figure 1, distinguishing kernel theories, meta-requirements, application principles, and testable design product

[14] An attempt to list all exceptional situations would lead to circular arguments, since if we tried to list all possible ordinary or exceptional situations, there would be "exceptional" situations in which this list would not apply. And then we would need additional application principles to solve these situations, and so on. Furthermore, when organizations face the same exceptional situations often enough the "exceptional situations" may become "ordinary," and they may be subsequently captured by IS security policies and guidelines (cf., Hare, 1981).

hypotheses. Since we do not suggest any IS security policies and guidelines, we omit meta-design from our analysis.

The Conservative Deontological Design Theory

The kernel theories of a conservative deontological design theory for IS security policies and guidelines are deontological moral theories. The design theory claims that what is not allowed by the IS security policies and guidelines is strictly rejected regardless of the consequences to which it would lead (see Table 3, point 3: Application principles). Thus, the meta-requirement is that IS security policies should list actions that employees must perform (Table 3: Meta-requirements). Employees should simply follow the list of dos and don'ts in the IS security policies and guidelines "religiously." The conservative deontological design theory is explicitly favored by David (2002 p. 510), for example.

Table 3. The Conservative Deontological Design Theory for IS Security Policies and Guidelines	
1. Kernel theories	Deontological moral theories.
2. Meta-requirements	IS security policies and guidelines must be comprehensive. IS security policies and guidelines must list all actions that employees must perform.
3. Application principles	Only the conventional level: follow the list of do's and don'ts literally.
4. Testable design product hypotheses	H1. The more comprehensive the IS security policies and guidelines are, the lower the TCSA. H2. The less voluntary it is for employees to follow the IS security policies and guidelines, the lower the TCSA.

The conservative deontological design theory implicitly assumes that the set of IS security policies should be as comprehensive as possible to define all allowable IS security actions. At the same time, it assumes that its application should be mandatory (non-voluntary). Yet no policy or guideline is absolutely mandatory, so employees could violate them if they decide to do so. In fact, each employee interprets a given IS security policy or guideline as mandatory to varying degrees (cf., Davidson, 1970). This links the hypotheses with the concept of "voluntariness" (Moore and Benbasat, 1991), and with the extant research on the impact of voluntariness on the acceptance of different IT artifacts (e.g., Iivari, 1996; Agarwal and Prasad, 1997; Karahanna, *et al*., 1999; Venkatesh, *et al*., 2003). Thus, the two testable design product hypotheses are: H1: the more comprehensive the IS security polices and guidelines are, the lower the total cost of Security Activities (TCSA); and H2: the more mandatory (i.e., less voluntary) the security policies and guidelines are, the more strictly enforced they will be, and the lower the TCSA will be.

The Liberal-Intuitive Design Theory

The kernel theory of a liberal-intuitive design theory for IS security policies and guidelines is libertarianism. According to liberal-intuitive design theory, those IS security actions that are not prohibited are allowed (Table 4). The first meta-requirement of this design theory differs from the conservative deontological design theory in that the liberal-intuitive design theory lists not all, but only the necessary actions that employees must perform. Liberal-intuitive IS security policies and guidelines are intended to be followed

literally; however, the meta-requirement is that if something is not covered by the IS security policy and guidelines, employees can take appropriate action to remedy the situation. The application decision is based on an employee's intuition.

Table 4. The Liberal-Intuitive Design Theory for IS Security Policies and Guidelines	
1. Kernel theories	Libertarianism, autonomy.
2. Meta-requirements	1: IS security policies must list the necessary or key actions that employees must perform. 2: If something is not covered by IS security policy and guidelines, employees can take appropriate action to remedy the situation.
3. Application principles	1. IS security guidelines are intended to be followed literally. 2. What is not explicitly denied is allowed. 3. If something is not covered by IS security policy and guidelines, follow your intuition.
4. Testable design product hypotheses	H3: The smaller the set of necessary IS security policies and guidelines are, the lower the TCSA. H4: The more mandatory (less voluntary) it is for employees to follow the necessary IS security policies and guidelines, the lower the TCSA.

The first meta-requirement that it is relevant to list only the very necessary IS security actions (Table 4) is very similar to the socio-technical design principle of minimal critical specification (Herbst, 1974). The principle of minimal critical specification in socio-technical thinking means that one identifies only the minimal set of conditions required to create viable, self-maintaining, and self-adjusting production units. As a consequence, the liberal-intuitive design theory includes the hypothesis (H3) that the smaller the set of critical (necessary) IS security policies and guidelines is, the lower the TCSA will be. This is essentially based on the assumption that employees' autonomy should be maximized, especially in situations not covered by the IS security policies and guidelines. However, the liberal-intuitive design theory presupposes strict compliance with the necessary IS security policies and guidelines. As a consequence, the second hypothesis claims that the more mandatory it is for employees to follow the critical IS security policies and guidelines, the lower the TCSA will be.

In exceptional situations, the liberal-intuitive design trusts employees' autonomy, suggesting that employees' self-determination and intrinsic motivation lead to better acceptance of IS security guidelines and policies, compared to extrinsic motivation to comply with IS security guidelines. Thus, the advocates of the liberal-intuitive design theory recognize that stressing employees' self-determination (employees' freedom to make their own decisions) may have weaknesses in terms of TCSA. These weaknesses relate to the permissive nature of the design theory: the fact that employees can exercise their own judgment may lead to potential risks from security and business perspectives. Despite such risks, advocates of the liberal-intuitive design theory consider that using minimal external impositions leads to better overall results in terms of TCSA.

The Prima-Facie Design Theory

The kernel theory of the *prima-facie* design theory for IS security policies and guidelines is based on Ross' (1930) *prima-facie* principles, taking the view that IS security policy and guidelines should be followed in normal situations. However, when solving conflicts in exceptional situations, the *prima-facie* design theory holds that IS security policies and guidelines can be formally violated, as long as the expected benefits of compromising those security guidelines (excluding a person's egoistic/ideological benefits) clearly outweigh the expected benefits of complying with the security guidelines, in terms of the TCSA (Table 5).

Table 5. The *Prima-Facie* Design Theory for IS Security Policies and Guidelines.	
1. Kernel theory	The prima-facie principles of Ross.
2. Meta-requirements	IS security policies must list all actions that employees must perform in normal situations.
3. Application principles	The conventional level and critical levels. Guidelines can be violated in exceptional situations if the expected benefits of compromising the guidelines outweigh the expected benefits of complying with the security guidelines in terms of TCSA.
4. Testable design product hypotheses	H5. The more comprehensive the IS security policies and guidelines are, the lower the TCSA will be in normal situations. H6. The less voluntary it is for employees to follow the IS security policies and guidelines, the lower the TCSA in normal situations. H7. The more voluntary it is for employees to follow the IS security policies and guidelines and the more the expected benefits of compromising those guidelines outweigh the expected benefits of complying with the security guidelines, the lower the TCSA in exceptional situations.

The *prima-facie* design theory includes Hypothesis H5, which states that the more comprehensive the IS security policies and guidelines are, the lower the TCSA will be in normal situations, and Hypothesis H6, which states that the more mandatory (less voluntary) compliance with IS security policies and guidelines is in normal situations, the lower TCSA will be. Hypothesis H7 assumes an interaction effect between voluntariness and expected benefits (expected benefits of compromising – expected benefits of complying): the more voluntary and the higher the net benefit, the lower TCSA will be.

The Virtue Design Theory

The kernel theories of the virtue design theory for IS security policies and guidelines are virtue ethics by MacIntyre (1987)—including the virtues of justice, courage, and honesty—and the thesis of supererogation. Thus, the meta-requirement of the virtue design theory states that IS security policies and guidelines are supererogatory, and describe the actions that virtuous employees follow.[15] However, actions in conflict with IS security policies and guidelines are not considered to be wrong, or punishable. The

[15] Here the IS security policy and guidelines are loosely interpreted as 'the standard', following MacIntyre's (1987) term.

application decision in resolving possible conflicts between security policies and business goals is made in light of the virtues (justice, honesty, and courage) – see Table 6.

Table 6. The Virtue Design Theory for IS Security Policies and Guidelines.	
1. Kernel theories	Virtue ethics and the thesis of supererogation in virtue ethics.
2. Meta-requirements	IS security policies and guidelines should list virtuous conduct.
3. Application principles	1. Obedience to IS security guidelines is not obligatory, though it is virtuous. 2. Virtuous actions, as defined by the IS security policy and guidelines, are welcomed, but not compulsory, in exceptional situations.
4. Testable design product hypothesis	H8. The more voluntary it is for employees to follow the IS security policies and guidelines, and the more virtuous (just, courageous and honest) the actions are, the lower the TCSA in exceptional situations.

The testable design product hypothesis, H8, referring to the virtuousness of actions, differs from the *prima-facie* design theory, which refers to the relative benefits of compromising and complying with IS security policies and guidelines.

The Utilitarian Design Theory

Utilitarianism is the kernel theory of the utilitarian design theory for IS security policies and guidelines. The utilitarian design theory suggests that, in general, IS security policies and guidelines should be followed (Table 7).

Table 7. The Utilitarian Design Theory for IS Security Policies and Guidelines.	
1. Kernel theory	Utilitarianism.
2. Meta-requirements	IS security policies must list all the actions that employees must perform in normal circumstances.
3. Application principles	1. Follow guidelines in normal circumstances. 2. Otherwise, the happiness of the greatest number of people and the absence of pain are the factors that count in deciding whether an action is allowable.
4. Testable design product hypotheses	H5. The more comprehensive the IS security policies and guidelines are, the lower the TCSA will be in normal situations. H6. The less voluntary it is for employees to follow the IS security policies and guidelines, the lower the TCSA in normal situations. H9. The more voluntary it is for employees to follow the IS security policies and guidelines, and the more happiness brought about by the actions of employees, the lower the TCSA in exceptional situations.

According to the utilitarian design theory, IS security policies and guidelines can be violated in special circumstances: they are to be compromised only if an act in violation of the security policy produces the greatest happiness, or good, for all the people affected by that action. Thus, the utilitarian design theory is similar to the *prima-facie* and

universalizability IS security policy design theories, in that they all recognize the need to allow for violation of IS security policies and guidelines, provided that this yields a more positive effect than would be produced by following the policies and guidelines. The utilitarian design theory views the happiness of the greatest number of people as the factor that counts in deciding whether an action is allowable (Table 7: Application principles). That is, the best action to minimize TCSA is that which maximizes overall happiness.

The first two testable design product hypotheses, H5 and H6, are identical to those of the *prima-facie* theory. Hypothesis H9 refers, however, to overall happiness rather than to benefits, as in the case of the *prima-facie* theory.

The Universalizability Design Theory

The kernel theory of the universalizability design theory for IS security policies and guidelines is the thesis of universalizability. This view holds that the requirements of IS security policies and guidelines should, in general, be met. However, if considered inadequate (e.g., the rules are conflicting or, in an exceptional situation, the actions specified in the IS security guidelines do not seem to produce the best results in terms of TCSA), the IS security policies and guidelines can be violated, provided that the violation satisfies the thesis of universalizability.

Table 8. Universalizability Design Theory for IS Security Policies and Guidelines

1. Kernel theories	Universalizability theories.
2. Meta-requirements	IS security policies must list all actions that employees must perform in normal circumstances.
3. Application principles	In normal circumstances, follow the standard IS security guideline. Otherwise, apply either of the two alternative universalizability principles: 1: Action Y is allowed if it is allowed for any X in the same or a similar situation; 2: If you were the security manager or the president of the organization, would you allow action Y by any trustworthy X?
4. Testable design product hypotheses	H5. The more comprehensive the IS security policies and guidelines are, the lower the TCSA will be in normal situations. H6. The less voluntary it is for employees to follow the IS security policies and guidelines, the lower the TCSA in normal situations. H10. The more voluntary it is for employees to follow the IS security policies and guidelines, and the more universalizable the actions (of employees) are, the lower the TCSA in exceptional situations.

The universalizability design theory has meta-requirements similar to the *prima-facie* and utilitarian design theories. However, the method used to solve possible conflicts or test the relevance of IS policies differs from those of the other design theories.

The universalizability thesis consists of two sub-theses: “security partial” and “impartial,” which are the two application principles for solving possible conflicts or testing the relevance of an IS policy. The impartial universalizability thesis states:

Action Y is allowed if it is allowed for any X in the same or similar situation.
The security/business objective partial universality thesis states:
If you were the security manager or the president of the organization, would you allow action Y by any trustworthy X?

X refers to any worker and Y to actions. Thus, in the case of the second (security partial universality) thesis, an employee considers whether, if he or she were the security manager or president, he or she would allow the action.

The first testable design product Hypotheses H5 and H6 are identical to the *prima-facie* and utilitarian design theories. In terms of Hypothesis H10, the universalizability thesis in a sense requires absolute universalizability. However, in practice, the action may be more or less universally accepted by the members of society. Therefore, Hypothesis H10 recognizes different degrees of universalizability, but, it can also be interpreted as a dichotomous variable (non-universalizable, universalizable), if so desired. Otherwise, Hypothesis H10 is analogous to the corresponding hypothesis of the *prima-facie*, virtues, and utilitarian design theories, the difference being that it refers to universalizability instead of benefits, virtuousness, or overall happiness.

Summary

The above analysis leads to the following classification of IS security policies and guidelines (Figure 2). The classification is based on the hypotheses generated in Tables 3-8. Conservative-deontological theory, on the one hand, and liberal intuitive and *prima-facie* design theories, on the other hand, represent opposite extremes.

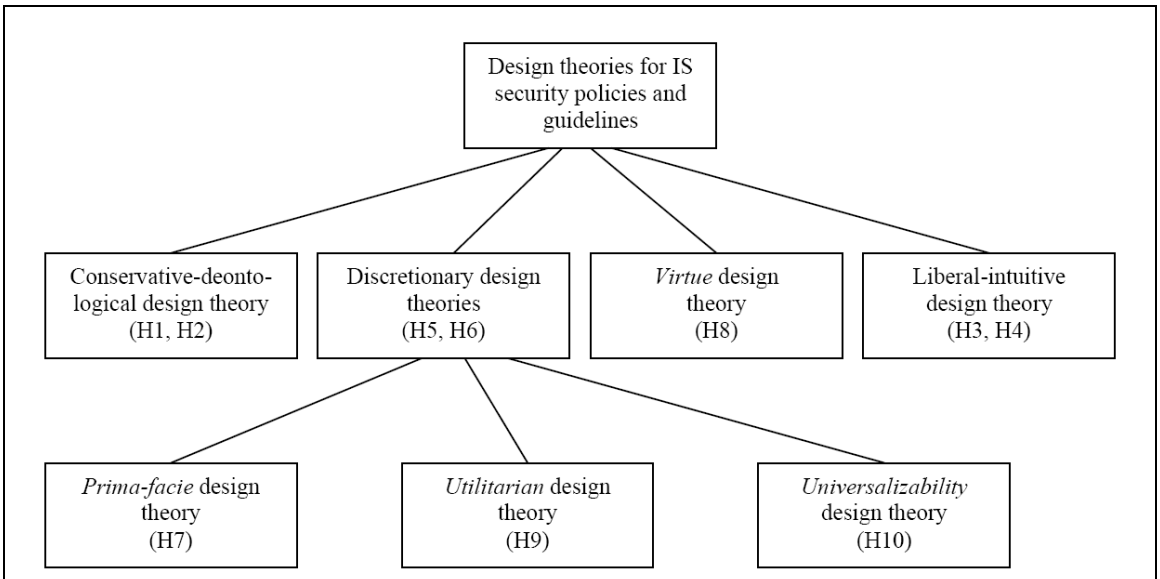

Figure 2. Classification of Design Theories for IS Security Policies and Guidelines

The other three design theories represent intermediate positions between the two extremes. They share Hypotheses H5 and H6, but each of them proposes different reasons and rationales for the violation of IS security policies and guidelines in exceptional situations.

Discussion

Implications for Practice

This paper proposes six design theories based on normative theories developed in philosophy to make sense of alternative views of application principles. These application principles are important for practitioners not only in the development of IS security policies and guidelines, but also in the application of these policies in different situations. The alternative positions affect how comprehensive the IS security policies and guidelines should be, and the ways in which exceptional situations are addressed.
The case of a Finnish scuba-diving site that helped Finnish victims and relatives after the North Sumatra tsunami in December 2004 (Nieminen, undated) illustrates the significance of the *prima-facie*, utilitarian, and universalizability design theories in an exceptional situation. Mr. Alex Nieminen, one of the administrators of the diving site, started to receive short messages from Finnish divers in Thailand soon after the catastrophe on December 26, 2004. As he received the messages pertaining to Finns who had been found alive in hotels and hospitals, Mr. Nieminen inserted their names on the website, www.sukellus.fi, providing information about survivors much earlier than the official Finnish authorities did.

However, what Mr. Nieminen did was illegal. According to Finnish law, it is illegal to post lists of names without the consent of the person in question. In fact, Nieminen was contacted on December 30 by Mr. Reijo Aarnio, the national ombudsman of information security in Finland. However, the Finnish government and the national ombudsman decided to ignore the information security law in this exceptional situation.

This example demonstrates the limitations of the conservative deontological design theory. First, practitioners need to be aware that compliance with IS security guidelines for their own sake may get in the way of unexpected business (or other) opportunities that require actions that conflict with the company's IS security policy. Second, while it attempts to cover all security issues in a security policy, the conservative deontological design theory can easily lead to excessive security and unnecessary bureaucracy (Madsen, 1995). Thus, we see that the conservative-deontological design theory is impractical in organizations that have high environmental uncertainty (Boyd and Fulk, 1996 p. 4; Daft, *et al*., 1988 p. 125), because of its inflexible nature. The more turbulent (having a fast rate of change), unpredictable and complex a business environment is, the more inadequate the conservative-deontological design theory is. Furthermore, the conservative-deontological design theory is postulated to be ineffective in organizations with instrumentally-oriented (employees are expected to do everything to further the company's interest, regardless of the consequences), caring-oriented (employees are expected to what is best for everyone), or independence-oriented (employees are expected to follow their own beliefs) cultural norms, as observed in an empirical study by Victor and Cullen (1998). On the other hand, the conservative-deontological design theory is expected to be effective in rule-oriented organizations where people are used to acting strictly by the book (Loch and Conger, 1996; Victor and Cullen, 1998).

The liberal-intuitive and virtue design theories are the two alternatives at the other extreme. Their potential strengths result from the freedom they bestow on employees. However, according to liberal intuitive thinking, this freedom would not have justified Mr. Nieminen's violation of the law in the case above, since liberal-intuitive design theory

allows actions only in those situations that are not covered by policies or laws. In the case of virtue design theory, actions in conflict with the IS security policies and guidelines are not considered to be wrong, or punishable, as long as they can be considered virtuous (just, honest and courageous). The action of Mr. Nieminen can be considered courageous and therefore acceptable.

The freedom allowed by treat two design theories may also be a security threat. The liberal-intuitive and virtue design theories rely on employees' intuition either directly (in the liberal-intuitive design theory) or through virtues (in the case of virtue ethics). These may be poor guides in the case of IS security issues.

The *prima-facie*, utilitarian, and universalizability design theories lie between the two extreme positions. The strength of these three design theories, compared to the conservative one, is their flexibility. They may lead to a better situation in terms of TCSA, particularly in exceptional situations. Another strength, compared with the liberal-intuitive and virtue design theories, relates to decision making and accountability in exceptional situations. The *prima-facie*, utilitarian, and universalizability design theories endeavor to offer more reliable application principles by placing certain restrictions on the employees' thinking through, for instance, the universality principle or utilitarian calculations. They all emphasize that one should have good reasons to violate the IS security policies and guidelines.

The possible weakness of the *prima-facie*, utilitarian, and universalizability design theories relates to the rules governing exceptions (application principles): that is, the factors that determine or justify the taking of an action that is in conflict with, or not covered by, the IS security policies and guidelines. In this respect, the *prima-facie* design theory stresses that the benefits of violating the guidelines must outweigh those of complying with the guidelines. However, this condition has its problems. For example, the sub-principle of the *prima-facie* design theory that states "the expected benefits of compromising the security guidelines (excluding a person's egoistic benefits) clearly outweigh the expected benefits of complying with the guidelines" means that the judgments devolve to the employees, and thus allow for subjective interpretations. For instance, the view of what constitutes "benefits" may vary from person to person. Similarly, the utilitarian application principles suggest choosing the course of action that maximizes the happiness of the greatest number of people. But it is not easy to measure others' happiness (Siponen and Vartiainen, 2001); and does such maximization of happiness necessarily lead to business success or security?

The universalizability design theory tries to overcome these weaknesses by enforcing impartiality (the first principle) and the viewpoint of the security manager (the second principle). But can employees ultimately know how the security manager or the president of the organization would think? However, the strength of this design theory is that it constrains employees to making decisions as if they were in the shoes of the security manager or the president of the organization. In other words, even though no one can know another's thoughts, the employees are required to do their best to maintain security from the security manager's or the president's point of view.

Despite all the difficulties discussed above, the actions of Mr. Nieminen can be justified in terms of the *prima-facie*, utilitarian, and universalizability design theories. His action responded to an enormous demand for information when the Finnish authorities were unable to provide such information. On December 27 the website had 76,581 visitors,

the next day 204,516 visitors, the following day 255,943 visitors, and on December 30,234,218 visitors, whereas the normal number of daily visitors was about 300. As a consequence, one can argue that the expected benefits of his illegal action far exceeded the expected benefits of complying with the law (*prima-facie* design theory). One can also argue that his illegal action of publishing the names of survivors brought about great happiness among people worried about their relatives and friends in the affected area in Thailand at the time of the tsunami (utilitarian design theory). It also seems that the national ombudsman of information security accepted Mr. Nieminen's action in this situation, suggesting that partial universalizability applied in this case.[16]

Research implications: A theoretical synthesis of the six design theories

The above example demonstrates that it is not always justifiable to stick literally to IS security policies and guidelines. In an exceptional situation, one may have a good reason to violate IS security policies and guidelines. The *prima-facie*, utilitarian, and universalizability design theories provide general ideas on how to justify the violations. One research problem is to produce empirical evidence as to how common various categories of "exceptional" situations (where IS security policies and guidelines conflict with business objectives) are in practice. A second research problem is to find out how people address such conflicting situations: whether they just follow the rules, or violate them in some way. If they violate the rules, a third research question is how do they rationalize their actions, referring to net benefits, virtuousness, happiness, or perhaps the universalizability of their actions? A fourth research question concerns the consequences of complying with and violating IS security policies and guidelines: how effective the different rationales suggested by the six design theories are in guiding people's actions.

Figure 3 presents a research model for the fourth research question. Its core is based on the ten testable design product hypotheses derived from the six normative theories (Tables 3-8, Figure 2). Referring to our discussion in section 5.1, we have also included some external factors just to emphasize the fact that we do not claim that Hypotheses H1-H10 tell the whole story. The purpose of the inclusion of the two external variables is not to propose any contingency theory that there is a fit between the external factors and the six design theories. The only purpose is to illustrate that the external factors may influence the relationships assumed by Hypotheses H1-H10. The dotted arrows from "Environmental turbulence" and "Organizational culture" depict the influence discussed in Section 5.1 in the context of the conservative deontological design theory. They are expected to moderate the effects as illustrated by the dotted lines.[17] The solid arrows from the two external variables remind one that these variables may also affect relationships in Figure 3 more generally.

[16] In this 'tsunami' case, we replaced the CEO/security manager with the national ombudsman.

[17] Figure 3 makes a distinction between interaction effects (shown as joining lines) and moderators (shown as arrows heading towards other arrows). The variables in the interaction effect have a symmetrical role as predictors, and there may be more than two predictor variables in the interaction term, whereas the variables in the moderator case are not symmetrical, and the moderator moderates an association between one predictor variable and one dependent variable.

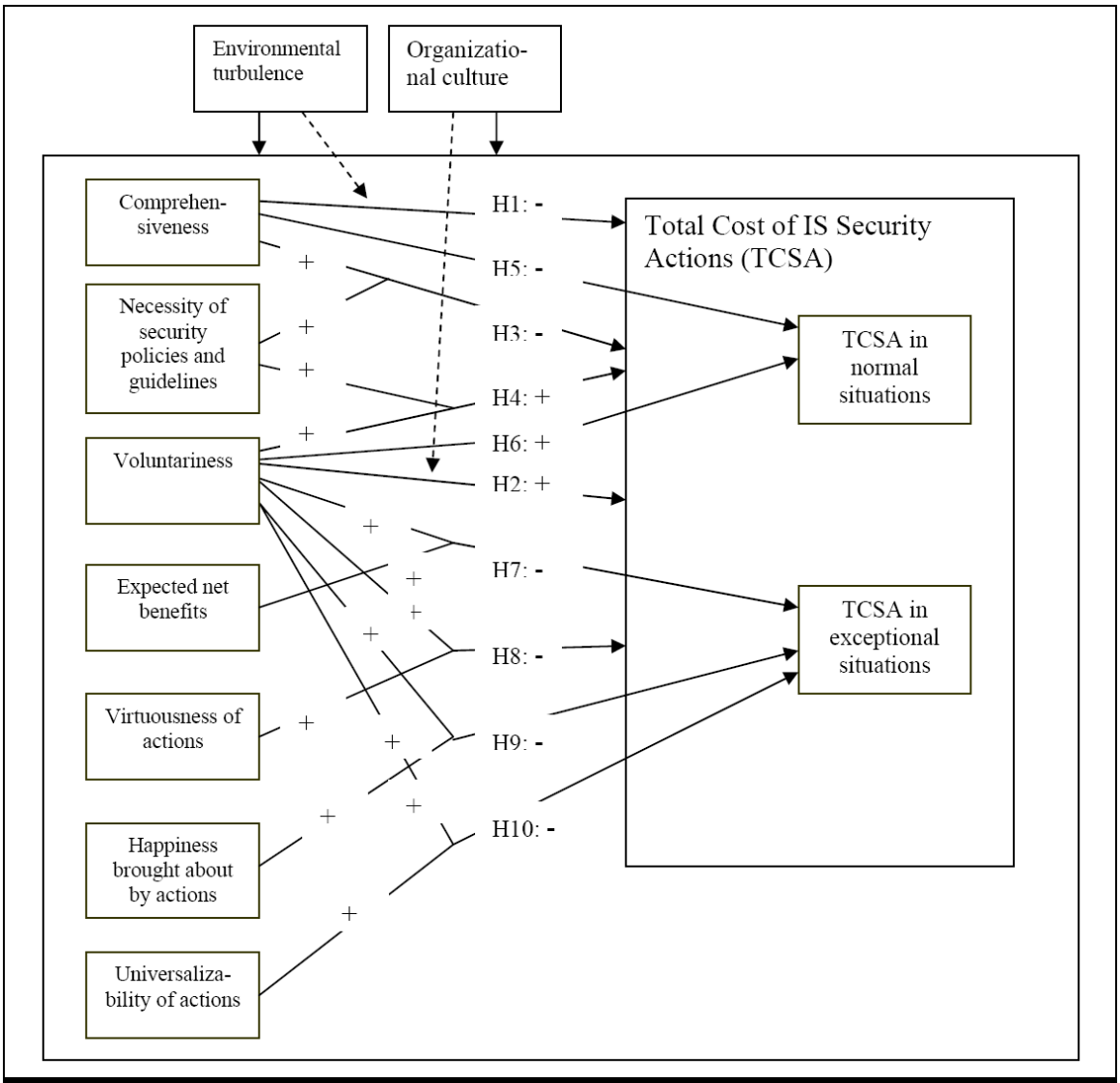

Figure 3. A Theoretical Synthesis of the Six Design Theories

Figure 3 focuses on the factors that explain the "success" of IS security policies and guidelines at the organizational level, the success being interpreted in terms of the Total Cost of Security Actions (TCSA). The +/- signs after the hypotheses describe whether the hypothesized relationship is assumed to increase or decrease the dependent variable. The +/-signs next to the independent variables on the left describe whether the influence of the dependent variable is an interactive relationship. For example, in the case of H7, the more voluntary and the higher the expected benefits, the lower the TCSA in exceptional situations.

As mentioned, the unit of analysis in Figure 3 is the organization. IS security policies and guidelines are, however, followed by individual employees. The individual adoption/acceptance of IS security policies and guidelines as a whole is another research topic, in which the different models of individual acceptance of IT artifacts, such as the Theory of Reasoned Action (Fishbein and Ajzen, 1975) and its extension to cover moral behavior (Loch and Conger, 1996 p. 75-76), the Theory of Planned Behavior

(Ajzen, 1991), the Technology Acceptance Model (Davis, 1989), and the Theory of Intrinsic Motivation (Deci and Ryan, 1985), can be utilized.[18] Since these are widely applied in IS, we will not discuss them here. Our only comment here is that the differences between the normative theories may also have implications for overall acceptance. For example, while seeking to cover all situations comprehensively, the conservative-deontological design theory easily results in a massive document of policies and guidelines that becomes complex and difficult to use. The other design theories (liberal-intuitive, *prima-facie*, utilitarian, universalizability) can be formulated in a more condensed way and, therefore, may be easier to use. On the other hand, some people may expect clear and definite policies and guidelines as exemplified by the conservative-deontological design theory, and may find the alternative design theories difficult to interpret and use.

Preliminary Ideas of Measuring the Constructs

The empirical testing of the model proposed in Figure 3 requires operationalization of the concepts, which for some may be tricky, though not necessarily impossible. While it is beyond the scope of the present paper to discuss these measurement issues at length, we will outline preliminary ideas as to how the constructs identified in the model can be measured.

Let us start with the easier constructs first. Organizational turbulence has been of considerable research interest in organizational contingency theory since the 1960s, leading to a number of measures (see Karimi et al., 2004, for a recent one). Although research into organizational culture has mostly been qualitative/idiographic, there have been some quantitative "measures" of it, too (e.g., Denison and Spreitzer, 1991; Hofstede, *et al*., 1990). In the case of voluntariness, we refer to Moore and Benbasat (1991) for a measurement instrument.

In the case of the comprehensiveness of IS security policies and guidelines, one can conceive of two methods of measurement. One option is to discover respondents' perceptions (preferably those of IS security experts) of this comprehensiveness using a number of items, for example, to what extent they agree with statements likes *"The totality of IS security policies and guidelines in my organization is comprehensive"* and *"Nothing essential is missing from the totality of IS security policies and guidelines in my organization."* The second option is to list all the potential IS security issues to be covered (perhaps based on an IS security checklist or set of standards, such as BS7799-1, 2000; GAISP, 2003; ISF, 2003; Wood, *et al*., 1987), and to ask, in the case of each issue, whether the organization's IS security policy and guidelines cover these issues.

The necessity of IS security policies and guidelines can easily be measured using perceptual measures such as to what extent the respondent agrees with the statements, *"IS security policy and guidelines are absolutely necessary in my organization"* and *"IS security policy and guidelines are absolutely critical in my organization."*

[18] Note that focus in Figure 3 is on individual decisions whether to follow IS security policies and guidelines rather than on the adoption/acceptance of the IS security policy as a whole. In fact, Figure 3 presumes this adoption/acceptance, but it does not require that an employee follows IS security policies and guidelines in all situations.

Let us proceed now to the more tricky constructs in Figure 3. One problem is that it may be difficult for the respondents to associate the philosophical concepts with actual practice. Therefore, in moral psychology, it is not unusual to tie up the questions with concrete problems through an imagined case – the moral dilemmas used by Kohlberg in his Theory of Cognitive Moral Development (Kohlberg, 1981) being a well-known example. Accordingly, one or more cases, such as the one presented in section 3.3., can be used to associate respondents' answers with concrete problems. As an illustration, we offer the following case (modified from the real case presented in section 3.3).[19]

Jack works in a software house, which has strict security rules laid down by a senior security specialist, who is regarded as the authority figure in security matters. The security policy includes a rule that states that passwords are personal and that one's password cannot be given to anybody else. Any exception must be approved by the senior security specialist. During the summer, while the senior security specialist and most of the developers are on their holidays, Jack and a few of his co-workers receive additional requirements for feature changes from an important customer. Jack needs to make changes to the software quickly in order to keep to the deadline. To do this, Jack needs to access some files to which he currently does not have access (access can be granted by a developer, who is on his holiday at that time, and the security specialist or his subordinates). Jack cannot reach the senior security specialist at that time, and the developer who has control over the files is also on holiday. He is available, but cannot remember his password any more (he forgot it while on holiday). Jack contacts Matt, who is a subordinate of the senior security specialist, but Matt wonders if he dares to violate the IS security policy of the organization. If Matt does not grant access to Jack, the result is that the software company will miss the deadline, which further results in the software company having to compensate the client financially. This may further damage the reputation of the software company, which in turn may reduce future contracts, and lead to other consequences.

After having read the example, the respondents can be asked to answer a number of questions, imagining that they are confronted with this problem in real life, in Matt's position. The questions might include, for example, to what extent he or she agrees with statements such as *"If I were absolutely sure that the benefits of violating the IS security policy and guidelines in the example situation would exceed the costs, I would be ready to violate the policy and guidelines"* and *"If I knew that the benefits of the violation would far exceed the costs, I would be ready to violate the policy and guidelines."*

The example above may best illustrate expected benefits and costs (*prima-facie* design theory). One could imagine analogous examples that might identify the virtuousness, happiness, and universalizability of actions. In each case, one could present similar questions: *"If I knew that violation of IS security policy and guidelines in the example situation represented just and honest action, I would be ready to violate the policy and guidelines," "If I knew that violation of IS security policy and guidelines in the example situation would bring happiness to the people affected (such as employees, customers, and stakeholders of the organization), I would be ready to violate the policy and guidelines,"* and *"If I knew that the CEO of the organization would accept the violation of the security policy in the example situation, it would encourage me to violate the policy."*

[19] Of course, it would be better if the imagined case could be rooted in each respondent's own organization.

Summary

Existing studies on IS security policies pay little attention to how to deal with exceptional situations in which IS security policies are in conflict with the business objectives of organizations. To fill this gap, this paper first develops an IS security design theory framework, and then proposes six kernel theories with distinctive application principles by which such conflicts can be resolved. These six kernel theories are: the conservative-deontological, liberal-intuitive, *prima-facie*, virtue, utilitarian, and universalizability normative theories. Based on these, we derived six normative design theories for IS security policies and guidelines. The conservative-deontological design theory was argued to be suitable only in stable business environments and in rule-oriented organizations (where people are accustomed to acting by the book). Outside of rule-oriented organizations, and in a turbulent business environment, it is advisable to adopt the *prima-facie*, the virtue, the utilitarian, or the universalizability design theory. These six design theories were synthesized into a theoretical model. Once tested empirically, the results will lead to new insights on the extent to which IS security policies and guidelines should be backed by expected net benefits, virtuous actions, happiness, and unversalizability. This will help organizations to design effective IS security policies and guidelines in practice.

References

Agarwal, R. and Prasad, J. (1997) "The role of innovation characteristics and perceived voluntariness in the acceptance of information technologies," *Decision Sciences*, 28(3), pp. 567-582.

Ajzen, I. (1991) "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*. 50, pp. 179-211.

Baskerville, R. (1995) The Second-Order Security Dilemma. In W. Orlikowski, G. Walsham, M. Jones and J. DeGross (Eds.) Information Technology and Changes in Organizational Work. London: Chapman & Hall, pp. 239-249.

Baskerville, R. and Siponen, M. (2002) "An Information Security Meta-policy for Emergent Organizations," *Journal of Logistics Information Management*, special issue on Information Security, 5-6, pp. 337-346.

Bentham, J. (1876) An introduction to the principles of morals and legislation, Clarendon Press, Oxford, UK.

Boyd, B. and Fulk, J. (1996) "Executive scanning and perceived uncertainty: a multidimensional model," Journal of Management, 22(1), pp. 1-21.

Broderick, J.S. (2001) "VPN Security Policy," Information Security Technical Report, 6(1), pp. 31-34.

BS7799-1 (2000), Code of Practice for Information Security Management, Department of Trade and Industry.

Code of Practice for Information Security Management, BS7799 (1993), Department of Trade and Industry. DISC PD003. British Standard Institution, London, UK.

Corby, M.J. (1999) Policy development. In: M. Krause and H.T. Tipton (eds): Handbook of Information Security Management, CRC Press LLC, FL, USA, Pp. 403-422.

Daft, R.L., Sormunen, J., and Parks, D. (1988) "Chief executive scanning, environmental characteristics, and company performance: an empirical study," *Strategic Management Journal*, 9(2), pp. 123-139.

David, J. (2002) "Policy enforcement in the workplace," *Computers & Security*, 21(6), pp. 506-513.

Davidson, D. (1970) "How is Weakness of the Will Possible?," in Joel Feinberg (ed.), *Moral Concepts*. Oxford: Oxford University Press.

Davis, F. (1989), Perceived usefulness, perceived ease of use, and end acceptance of information technology. MIS Quarterly, Vol. 13, no. 3, September, pp. 319-340.

Deci, E.L. and Ryan, R. M. (1985), Intrinsic Motivation and Self-determination in human behavior. Plenum Press. New York. USA.

Denison, D.R. and Spreitzer, G.M. (1991) "Organizational culture and organizational development: A competing values approach," in Woodman, R.W. and Pasmore, W.A (eds.), *Research In Organizational Change and Development*, Volume 5, JAI Press Inc, Greenwich, CT, pp. 1-21

Dhillon, G. (1997), Managing Information Systems Security. MacMillan Press LTD, UK.

Dhillon G and Backhouse J (2000) Information system security management in the new millennium. Communications of the ACM, vol. 43, no. 7, pp. 125-128.

Dhillon, G., and Backhouse, J. (2001) "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal*, 11(2), pp. 127-154.

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

Floridi, L. (1999), "Information Ethics: On the Philosophical Foundation of Computer Ethics," *Ethics and Information Technology*, 1(1), pp. 37-56.

Friedl, W.J. (1990), The computer security framework. Proceedings of the IEEE 1990 International Carnahan Conference on Security Technology, Lexington, KY, USA.

Fulford, H. and Doherty, N.F. (2003) "The application of information security policies in large UK-based organizations: an exploratory investigation," *Information Management & Computer Security*, 11(3), pp. 106-114.

GAISP (2003), Generally Accepted Information Security Principles (GAISP). Version 3.0. http://www.issa.org/gaisp/_pdfs/v30.pdf.

Habermas, J. (1990) Moral Consciousness and Communicative Action, Cambridge, UK: Polity.

Hale, R. (1996) "End-User Computing Security Guidelines," *Information System Security*, 6(1).

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

Hare, R. M. (1963) Freedom and Reason. Clarendon Press, Oxford, UK.

Hare, R.M. (1981) Moral Thinking: its levels, methods and point. Clarendon Press, Oxford, UK.

Hare, R.M. (1996) "Hare: A Philosophical Self-Portrait," In T. Mautner (eds): A Dictionary of Philosophy, Blackwell publisher ltd., UK, pp. 177-178.

Hare, R.M. (1997) "A Taxonomy of Ethical Theories," In R.M. Hare (eds): Sorting out Ethics. Oxford University Press, UK.

Hare, R.M. (1999) Objective Prescriptions and other Essays, (eds.): R.M. Hare. Oxford University Press, Oxford, UK.

Herbst, P.G. (1974) Socio-Technical Design, Strategies in Multidisciplinary Research, Tavistock Publications, London, UK.

Hevner, A.R., March, S.T., Park, J., and Ram S. (2004) "Design Science in Information Systems Research," MIS Quarterly, 26(4), pp. 75-105.

Hickson, N. (1997), Encryption policy — A UK perspective, 16(7), pp. 583-589.

Hofstede, G., Neuijen, B., Ohayv, D.D. and Sanders, G., "Measuring organizational cultures: A qualitative and quantitative study across twenty cases," *Administrative Science Quarterly*, 35, pp. 286-316

Hursthouse, R. (1996) "Normative Virtue Ethics.," In R. Crisp (ed.): How should one live? Oxford University Press, UK, pp. 19-36.

Höne, K. and Eloff, J. H. P. (2002) "Information security policy — what do international information security standards say?," Computers & Security, 21(5), pp. 402-409.

Iivari, J. (1996) "Why are CASE tools not used?," *Communications of the ACM*, 39(19), pp. 94-103.

ISF Standard of Good Practice for Information Security (2003). Available at http://www.isfsecuritystandard.com/index_ie.htm.

Kant, I. (1993) The Moral Law: Groundwork of the Metaphysic of Morals, Routledge, London.

Karahanna, E., Straub, D.W., and Chervany, N.L. (1999) "Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs," *MIS Quarterly*, 23(2), pp. 183-213

Karimi, J., Somers, T.M., Gupta, Y.P. (2004) "Impact of Environmental Uncertainty and Task Characteristics on User Satisfaction with Data," *Information Systems Research*, 15(2), pp. 175-193.

Karyda, M., Kokolakis, S., Kiountouzis, E. (2003), Content, Context, Process Analysis of IS Security Policy Formation. Proceedings of the IFIP TC11 18th International Conference on Information Security (SEC2003), May 26-28, 2003, Athens, Greece (SEC 2003), pp. 145-156.

Kohlberg, L. (1981) The Philosophy of Moral Development: Moral Stages and the Idea of Justice. Essays on Moral Development, Volume I. And Volume II: The Psychology of Moral Development: The Nature and Validity of Moral Stages Harper & Row, Publishers San Francisco. USA.

Kukathas, C. and Pettit, P. (1990) Rawls - A Theory of Justice and its Critics. Stanford University Press, California, USA.

Lindup, K. R. (1995) "A New Model for Information Security Policies," *Computer & Security*, 14(8), pp. 691-695.

Loch, K.D and Conger, S. (1996) "Evaluating Ethical Decision-Making and Computer Use," *Communications of the ACM*, 39(7), pp. 74-83.

Lupu, E.C., Sloman, M. (1999) "Conflicts in Policy-Based Distributed Systems Management," *IEEE Transactions on Software Engineering*, 25(6), pp. 852-869.

MacIntyre, A. (1987) After virtue: A Study in Moral Theory, Second edition, London, Duckworth, UK.

Mackie, J.L. (1981) Ethics, Inventing Right and Wrong, London: Penguin.

Madsen, W. (1995) "Reinventing federal security policy: A failed effort," *Information Systems Security*, 4(1).

Markus, M.L., Majchrzak, A. and Gasser, L. (2002), A design theory for systems that support emergent knowledge process. MIS Quarterly, vol. 26, issue 3, pp.

Mill, J.S. (1895), Utilitarianism. Routledge, London, UK.

Moore, G.C. and Benbasat, I. (1991), Development of an instrument to measure the perceptions of adopting information technology innovation, Information Systems Research 2(3), pp. 192-222

Nieminen, A. (undated). Sukellus.fi: Viikko Aasian maanjäristyksen jälkeen (http://www.sukellus.fi/archives/000194.shtml, accessed 26.05.2006)

Nosworthy, J.D. (2000) "Implementing Information Security In The 21st Century — Do You Have the Balancing Factors?," *Computers & Security*, 19(4), pp. 337-347.

Olnes, J. (1994) "Development of Security Policies," *Computers & Security*, 13(8), pp. 628-636.

Osborne, K. (1998) "Auditing The IT Security Function," *Computers & Security*, 17(1), pp. 34-41.

Palmer, M.E. Robinson, G., Patilla, J, and Moser, E.P., (2001) "Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age," *Information Systems Security*, 10(2).

Parker, D. B. (1997) "Information Security in a Nutshell," *Information System Security*, 6(1).

Pounder, C. (1997) "First Steps Towards a European Union Policy on The Securing of Electronic Communications," *Computers & Security*, 16(7), pp. 590-594.

Pounder, C. (2001) "The European Union Proposal for a Policy Towards Network and Information Security," *Computers & Security*, 20(7), pp. 573-576.

Pounder, C. (2002) "Security policy update," *Computers & Security*, 21(7), pp. 620-623.

Puhakainen, P. (2006) "A Design Theory for Information Security Awareness", Ph.D. Thesis, Faculty of Sciences, the University of Oulu, Oulu University Press, Finland.

Ross, D. (1930), The Right and the Good. Oxford University Press, UK.

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

Siponen, M.T. (2005) "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods," *Information and organization*, 15(4), pp. 339-375.

Siponen, M.T. and Vartiainen, T. (2002) "Teaching End-User Ethics: Issues and a Solution Based on Universalizability," *Communications of the Association for Information Systems*, 8(29), pp. 422-443.

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

Stevenson, C. L. (1944) Ethics and Language, New Haven: Yale University Press.

Straub, D. W. (1990) "Effective IS Security: An empirical Study," *Information System Research*, 1(2), pp. 255-277.

Strong, D.M. and Miller, S.M. (1995) "Exceptions and exception handling in computerized information processes," *ACM Transaction on Information Systems*, 13(2), pp. 206-233

Truex, D., Baskerville, R. and Klein, H. (1999), Growing Systems in Emergent Organizations. Communications of the ACM 42(8), pp. 117-123.

Twining, W. and Myers, D. (1999), How to do things with rules. Fourth Edition, Butterworths, London.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, Vol. 27, No. 3, pp. 425-478

Walls, J.G., Wildmeyer, G.R., El Sawy, O.A. (1992), Building an Information Systems Design Theory for Vigilant EIS. Information Systems Research, vol. 3, no, 1, pp. 36-59.

Walter, J.E. (1993) Security in unattended computing labs—safeguarding users as well as machines. Proceedings of the 21st annual ACM SIGUCCS conference on User services, San Diego, CA.

Warman, A.R. (1992) "Organizational computer security policy: the reality," *European Journal of Information Systems*. 1(5), pp. 305-310.

Victor, B. and Cullen, J. B. (1988) "The organizational bases of ethical work climates," Administrative Science Quarterly 33(1), pp. 101-125.

Wood, C.C. (1995) "Writing InfoSec Policies," *Computer & Security*, 14(8), pp. 667-674.

Wood, C.C. (1996a) "Constructing difficult-to-guess passwords," *Information Management & Computer Security*, 4(1), pp. 43-44.

Wood, C.C. (1996b) "A computer emergency response team policy," *Information Management & Computer Security*, 4(2).

Wood, C.C. (1996c) "A Policy for sending secret information over communications networks," *Information Management & Computer Security*, 4(3).
Wood, C.C. (1997a) "Part of the foundation for secure systems: separation of duties policy," *Information Management & Computer Security*, 5(1), pp. 18-19.
Wood, C.C. (1997b) "A secure password storage policy," *Information Management & Computer Security*, 5(2), pp. 79-80.
Wood, C.C. (1997c) "Policies alone do not constitute a sufficient awareness effort," *Computer fraud & security*, pp.14-19
Wylder, J.O. (2003) "Improving Security from the ground up," *Information Systems Security*, pp. 29-38.

About the Authors

Mikko Siponen is a Professor in the Department of Information Processing Science at the University of Oulu, Finland. He received his Ph.D. in Information Systems at the University of Oulu, and his DSSc in applied philosophy at the University of Joensuu. His research focus is on IS security, IS development and ethical aspects of IS. His research work has been published in journals such as *Information and Organization*, *Communications of the ACM*, *European Journal of Information Systems*, *IEEE magazines*, *Information Systems Journal and Data Base*. Dr. Siponen has received several academic awards, including the outstanding paper award in the 2000 volume of Information Management & Computer Security.

Juhani Iivari is a Professor in Information Systems at the University of Oulu, Finland. He is the Scientific Leader of the INFWEST Postgraduate Education Program of six Finnish Universities in the area of information systems. He received his M.Sc. and Ph.D. degrees from the University of Oulu, and served as the national coordinator of the Finnish Doctorate Programme in Information Systems 1993–94. His research focuses on theoretical foundations of information systems, information systems development methodologies and approaches, organizational analysis, implementation and acceptance of information systems, and the quality of information systems. Dr. Iivari has published in journals such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Omega*, *Communications of the ACM*, *European Journal of Information Systems*, *Information & Management*, *Data Base*, *Information and Software Technology*, *Information Systems*, *Information Systems Journal*, *Journal of Organizational Computing and Electronic Commerce*.

Journal of the Association for Information Systems
ISSN: 1536-9323