Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2013 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-18-2013

One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions

Mari Karjalainen
University of Oulu, mari.j.karjalainen@oulu.fi

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

Petri Puhakainen
Finnish Tax Administration, petri.puhakainen@vero.fi

Suprateek Sarker
Washington State University, sarkers@wsu.edu

ONE SIZE DOES NOT FIT ALL: DIFFERENT CULTURES REQUIRE DIFFERENT INFORMATION SYSTEMS SECURITY INTERVENTIONS

Mari Karjalainen, Department of Information Processing Science, University of Oulu, Finland, mari.j.karjalainen@oulu.fi

Mikko Siponen, Department of Computer Science and Information Systems, University of Jyväskylä, Finland, mikko.t.siponen@jyu.fi

Petri Puhakainen, Finnish Tax Administration, Finland, petri.puhakainen@vero.fi

Suprateek Sarker, Department of Management, Information Systems, and Entrepreneurship, Washington State University, US, sarkers@wsu.edu

Abstract

Employees' non-compliance with information systems (IS) security policies is a key concern for organizations. Previous studies have proposed different explanations for employees' behavior, such as the use of sanctions and monitoring, fear appeal and training, which represent different paradigms of learning. Previous works do not test the validity of their models or methods across different cultural settings. Based on interviews in four countries, we argue that while information security behaviors are learned, different paradigms of learning are effective in different cultures; i.e., different cultures require different IS security interventions. What is even more important is that by providing non-preferred IS security interventions (e.g., monitoring/sanctions in Switzerland) were negative for improving information security.

This study has implications for IS security research, editors, and practitioners. For scholars, we urge them to not only validate, but also test their models in different countries. The implication for editors is the need to re-consider their reviewing policy and accept papers that also show the limits of their model (not positive results) in some countries. From a managerial perspective, our findings suggest that different cultures require different IS security interventions.

Keywords: IS Security Behavior, IS Security Training, Culture

1 INTRODUCTION

The increased processing of sensitive information in organizations has brought information security issues to the forefront. One widely reported information systems (IS) security issue is employee non-compliance with IS security procedures (Johnston & Warkentin 2010). To help organizations address this concern, scholars have introduced different factors or variance models aimed at explaining or predicting employee compliance with IS security procedures (Bulgurcy et al. 2010; Herath & Rao 2009a; Johnston & Warkentin 2010; Siponen & Vance 2010). In addition, scholars have examined the means by which employees' intentions and behaviors can be changed (Johnston & Warkentin 2010; Puhakainen & Siponen 2010). While these studies have increased our understanding of employee compliance and how it can be improved, they do not test the validity of their models or methods across different cultural settings. In other areas of IS, cultural differences are common. To give one example in the IS security context in terms of power distance (Hofstede 1991)—how people accept/expect a hierarchical order in a society—it could be argued that in the high-power distance cultures, employees prefer behavioristic teacher-centered training where teachers are expected to take all initiatives in class, and students are comfortable with obeying the behavioral rules and norms expressed by the teacher. In turn, in the low-power distance cultures, employees could prefer student-centered approaches characterized by reciprocal communication and shared expertise between the "teacher" and employees (Karjalainen & Siponen 2011). Since organizations are becoming increasingly global and multicultural, there is a need to ensure the proposed means are effective in different cultural settings. Given that previous research has not examined this idea, this study contributes to the current IS research and practice by explaining how different approaches are effective in different cultures for changing employees' IS security behavior.

Our results are relevant to scholars and practitioners alike. For scholars, our results highlight the need to understand as well as further research the role of culture in employee compliance with IS security procedures. For practitioners, our results show that different cultures need different methods for changing employee IS security behavior, and point out practices that are expected to work in different countries.

The rest of this paper is organized as follows. The second section discusses the concept of culture and learning paradigms that form the basis for the study, and points out the lack of previous work on the influence of employees' cultures. The third section discusses the research methods, while the fourth section presents the results. The fifth section highlights the key findings and presents implications for future research and practice.

2 PARADIGMS OF LEARNING AS THEORETICAL SENSITIVITY AND PREVIOUS WORK ON IS SECURITY BEHAVIOR

This section introduces the concept of culture and discusses the paradigms of learning (Hung 2001; Miller & Seller 1985), and finally notes that previous works propose different means for influencing employees' IS security behavior, which present different paradigms of learning. Previous works do not discuss, however, whether their proposed means are effective in different cultural settings.

2.1 Culture

Two key questions in cultural research are the following: what is the underlying cultural theory and how does one define culture (Straub et al. 2002)? With respect to the former, much of the IS research on culture has applied Hofstede's theory (Myers & Tan 2002; Walsham 2002). While we are not denying the value of Hofstede's theory, previous research is rather critical of it (see Myers & Tan 2002; Walsham 2002). One of the critiques is that a score on, say, the scale of masculinity or uncertainty avoidance in terms of Hofstede's theory may be disconnected to specific context issues, such as employees' compliance with IS security procedures (Walsham 2002). From a theory-development perspective, besides knowing that individuals in a certain country tend to score high on

masculinity, it would be equally important to know what is culturally specific in IS security behavior in different countries. Obviously, Hofstede's theory cannot provide such context-specific knowledge. For this reason, we study employees' IS security behavior in different cultures inductively, following the work of Walsham (2002).

The definition of culture is a controversial issue. For example, Kroeber et al. (1952) present 164 definitions of culture. In the IS literature, Leidner and Kayworth (2006) note that culture may be defined by cultural artifacts such as norms, practices (Delong & Fahey 2000; Hofstede 1998), symbols (Burchell et al. 1980), individual belief systems, individual or corporate values, and cultural artifacts (Schein 1985). Straub et al. (2002) provide three categories of culture definitions.

For our study, we adopt the definition of Walsham (2002, p. 362), who defines culture as "*as shared symbols, norms, and values in a social collectivity such as country*," noting, however, that national cultures are composed of different people. As a result, Walsham (2002) maintains that there are individual differences within each cultural context. Another important point is that while culture is a group-level phenomenon, it manifests itself through the individuals, and hence culture can be assessed at an individual level (Straub et al. 2002).

One common assumption among the different definitions of culture is the idea that cultural assumptions are learned and, hence, can be changed (Schein 1985; Straub et al. 2002; Walsham 2002). This assumption has an important role in our study, and it is consistent with the paradigms of learning (Hung 2001; Miller & Seller 1985), which are illustrated in the next section and presented in Table 1.

2.2 Paradigms of Learning

Learning paradigm	**Behaviorism**	**Cognitivism**	**Constructivism and social constructivism**
Objective	Reception and mastery of pre-defined contents as objective knowledge	Development of cognitive abilities and problem-solving skills	Transformation of predominant beliefs and actions; personal or communal change
Teaching/learning methods	- Instructor-led approaches in order to transmit knowledge - Imitation or observational learning - Providing external reinforcement: punishments and rewards	Focuses on cognitive problem solving and analysis	Focuses on critical reflection of knowledge through collaboration or authentic problem solving
Examples of each paradigm of learning	- Reading or listening to formal presentations - IS security campaigning - Fear appeal campaign	- Using real-world examples of relevant assets, threats, and IS security accidents - Asking questions - Using emotions in learning	- Discussing employees' experiences, attitudes, and behaviors towards IS security policies - Learning through experience and experienced IS security accidents - Active acquisition and personal interest towards IS security-related knowledge - Involvement of IS

			security issues

Table 1. Paradigms of learning (e.g., Hung 2001; Miller & Seller 1985)

2.2.1 Behaviorism

The objective of behavioristic learning is to convey certain predefined contents, knowledge, facts, skills, concepts, and values to learners (Miller & Seller 1985). One-way communication through reading or listening without opportunities to reflect on the information is characteristic of behaviorism (Miller 2007). In the context of IS security training, using behavioristic teaching methods involves the teacher presenting IS security policies or information security threats and prevention activities to learners through different audiovisual means (e.g., face-to-face presentations and computer-based presentations). This is done without paying attention to the learning processes, problem-solving assignments (cognitivism), or individual or communal reflections on experiences (constructivism and social constructivism). Therefore, the content is presented to employees through reading or listening to formal presentations.

The behavioristic learning paradigm assumes that people learn through role models, a model that is based on imitation or observational learning (e.g. Bandura 1977). Hence, changing behaviors by following the role model of management can be seen as a behavioristic method.

The behavioristic learning paradigm also assumes that the learner's responses can be shaped through instructional procedures, such as reinforcement (Palincsar 1998). This means the learner's desired behavior is strengthened through monitoring behavior and offering positive reinforcement or punishments (Skinner 1969). Therefore, changing IS security beliefs through behavioristic methods involves changing behaviors through monitoring, punishments, and rewards.

2.2.2 Cognitivism

While behaviorism stresses the importance of the effective delivery of knowledge, imitation, and reinforcement in changing behaviors, cognitivism focuses on the mental activities of the learner and the efficient processing of knowledge (Hung 2001). Examples of cognitive learning methods include receiving reasons for compliance with IS security procedures, using real-world examples of relevant assets, threats, and IS security accidents, asking questions, and using emotions in learning.

2.2.3 Constructivism and social constructivism

The essential feature of constructivist and social constructivist learning is making connections between employees and the real world while making employees aware of their thinking processes. This idea maintains that learning occurs by critically reflecting on information through authentic problem solving and communication (Miller & Seller 1985). Learning requires interaction, negotiation, and collaboration (Palincsar 1998). When a person or group critically reflects, they question the validity of their actions and thoughts in order to change their perspectives (Mezirow 1991). To apply social constructivism to the context of IS security training, teaching methods should involve discussing employees' experiences, attitudes, and behaviors towards IS security policies. Such discussions are the foundation of collaborative learning, and must be planned to achieve mutual understanding and agreements on how to implement security policies in daily work. While behaviorist and cognitivist learning is directed by the external environment (e.g., organizational control, the trainer), constructivism stresses the active role of the learner in constructing new knowledge either individually or in collaboration with other people (Hung 2001). In the context of this research, (social) constructivist learning methods include problem-solving activities, learning by doing, reflecting on received knowledge, learning through experience, active acquisition, personal interest towards IS security-related knowledge, communication, discussion, and involvement.

2.3 Previous research on employee compliance with IS security procedures and IS security training

Based on the paradigms of learning introduced in the previous section, the extant empirical literature is divided into three research areas: (1) studies reflecting behavioristic learning, (2) studies reflecting cognitive learning, and (3) studies reflecting constructivist and social constructivist learning. All three of these research areas offer different perceptions of why employees comply with IS security procedures and how their behavior can be changed in an organizational context, and are based on empirical research and/or theories of learning.

Typically, behavioristic training emphasizes the instructor's activity or external reinforcement, leaving no room for active learning experiences (e.g., problem solving and critical reflection through communication). Studies reflecting on such behavioristic learning in the field of IS security behavior (1) report the influence of sanctions, rewards, or monitoring on employees' IS security behavior (Beautement et al. 2009; Bulgurcy et al. 2010; D'Arcy et al. 2008; Herath & Rao 2009a; 2009b; Li et al. 2010; Myyry et al. 2009; Siponen et al. 2007; Stanton et al. 2005). However, some research reports an insignificant effect between monitoring, sanctions, and/or rewards, and IS security behavior (Herath & Rao 2009a, 2009b; D'Arcy & Hovav 2007; Li et al. 2010; Pahnila et al. 2007; Siponen & Vance 2010). In addition, Johnston and Warkentin (2010) present the influence of fear appeals on employees' IS security behavior.

Besides punishments, rewards, and monitoring, the behavioristic learning approaches also assume that people learn through role models, a theory that is based on imitation or observational learning (e.g. Bandura 1977). Following this idea, Johnston and Warkentin (2010) and Dinev et al. (2009) write that social conformity, in terms of perceptions of peers and managers' expectations and attitudes, has an influence on employees' behavioral intentions to use anti-spyware software. Similarly, with social conformity, management and/or co-workers' attitudes and behavioral expectations or peer behavior (Chan et al. 2005, Herath & Rao 2009a, 2009b, Pahnila et al. 2007; Siponen et al. 2006) have been shown to have an influence on employees' IS security behavior.

Second, the studies reflecting cognitive learning in the field of IS security behavior (2) recognize the activation of learners' cognitive processing of information. Studies under this research area explain employees' IS security behavior through cognitive issues such as cognitive load (Beautement et al. 2009), failure to recognize the characteristics of human memory, unattainable or conflicting task demands, and lack of motivation (Sasse et al. 2001), cognitive processing (i.e., recognizing, understanding, and evaluating persuasive arguments) (Puhakainen & Siponen, 2010), and the connectedness of students' knowledge structures (Greitzer et al. 2007).

Finally, studies reflecting constructivist or social constructivist learning (3) are learner- or community-centered, which means that learners need to reflect on their own reasons for behaviors and attitudes for becoming more security-conscious. IS security studies in this area indicate that involving users through dialogue, participation, and collective reflection is a requisite for effective IS security training (Albrechten 2007; Albrechtsen & Hovden 2010). Similarly, Karjalainen and Siponen (2011) introduce experiential and collaborative approach for IS security training. The importance of employees' involvement in their organization's IS security issues is also recognized by Lee et al. (2004).

While all the aforementioned studies have been carried out in a single country, Hovav and D'Arcy (2012) added culture to their extended deterrence theory. They examined whether the deterrent effect of IS security practices, such as IS security policies, training, and monitoring, is influenced by culture in the United States and South Korea in the context of employee misuse of email and access rights. However, they did not collect actual cultural data, but they used the original Hofstede scores as a moderator. While the Hovav and D'Arcy (2012) study examined the organizational context, Dinev et al. (2009) built a model of the home-user context, specifically anti-spyware technology. This model expanded the theory of planned behavior using an integrated model of user acceptance of e-commerce (Pavlou and Fygenson 2006), adding the cultural dimensions identified by Hofstede (1993; 2001). They also performed a cross-cultural comparison between South Korea and the United States.

However, like Hovav and D'Arcy (2012), Dinev et al. (2009) did not collect data about the cultures, but simply used Hofstede's dimensions (and with standard scores) as moderators.

To conclude this literature review, while previous studies on employee IS security behavior and IS security training have pointed out the need to study the role of culture in information security behavior (Hovav & D'Arcy 2012; Dinev et al. 2009), none of these studies have examined the role of culture in employee compliance with IS security procedures across cultures in a specific, intensive manner (see Walsham 2002).

3 RESEARCH METHODS

3.1 Data collection

Empirical data collection was carried out in multiple locations of a global company (Company Globalcomp, a pseudonym), which operates in the marine industry and the energy market. The selected interview locations were Finland, Switzerland, the UAE, and China. These four locations were selected as representative of different cultural settings with the assistance of the information security manager of the organization.

Empirical data were collected through semi-structured qualitative interviews. To avoid a situation in which only certain groups of employees in an organization were interviewed, and to make sure the data represented the views of the whole organization (Myers & Newman 2007), the interviewees were selected from different organizational positions. Altogether, 80 face-to-face interviews were conducted between June and November of 2009. Of the 80 interviewees, 20 were Chinese (China), 15 were Western-European (Switzerland), 25 were Eastern-Asian (UEA), and 20 were Finnish (Finland). Interviewees in China and Finland were exclusively local employees. The respondents in Switzerland were originally from Germany (7), Austria (1), and Switzerland (7). The interviewees in the UAE were originally from India (15), Pakistan (4), Philippines (5), and Iraq (1). Fourteen interviewees were excluded from the analysis because they were originally from other countries, or their nationality was unclear (altogether, there were 94 interviews). The average interview length was 47 minutes.

When conducting interviews, it is important to note that the scholar's theoretical perceptions and perspectives do not drive the interview (Stinger 1999; Myers & Newman 2007), Therefore, the interviews were conversational in nature and involved a great deal of active listening to and understanding of the interviewees' construction of meaning rather than eliciting facts (Schulze & Avital 2011). Finally, it is important to ensure that interviewees feel that the information they reveal will not be used against them (Myers & Newman 2007). To address this issue, the interviewers carefully explained to the participants that the interview was confidential and that only the researchers were able to access the interview data. The interviewer also avoided presenting their own opinions on the research topic by emphasizing that there was no right or wrong response. Seventy-nine interviews were recorded and transcribed. Only one interviewee preferred the use of field notes.

3.2 Data analysis

Our research approach can be characterized as interpretative, qualitative, data-intensive, and inductive, with themes primarily derived from interviews (Walsham 2006).

Based on the interviewer's experiences during the interviews and the focus on our study, certain interview topics were selected for further examination. These topics were related to cultural differences in employee IS beliefs, how these behaviors are formed, and how they can be changed. The interview transcripts were analyzed by reading them as a whole and systematically searching a list of concepts related to management's role and how people learn new IS security procedures. A constant comparative approach to data analysis was followed. Based on this analysis, which was conducted by two researchers, general trends showing the common and different features among the four cultures were identified. The results of the study are discussed in Section 4.

4 RESULTS

Our study presents culture-independent and culture-dependent reasons for employees' IS security behavior (Table 2).

Culture-independent reasons	- Include previous work experience, work environment, professional identity, media, other people, social conformity, and active organizational IS security communications		
Culture-dependent reasons	**Behaviorism** Typical learning paradigm for interviewees in China and the UAE: - Behaviorist learning methods were preferred: one-way delivery of knowledge - Employees' IS security behavior is positively influenced by authority - People learn through imitation or observation of management's actions - Punishments, rewards, and monitoring were considered effective methods	**Cognitivism** No clear cultural differences	**Constructivism and social constructivism** Typical learning paradigm for interviewees in Finland and Switzerland: - Constructivist learning methods were preferred: active role of the learner in constructing knowledge either individually or in collaboration with other people - Emphasis of the personal responsibility of each individual employee instead of management's support - Monitoring of employees was considered ineffective method and had a negative effect on behavior

Table 2: Summary of the results of the study

4.1 Culture-independent reasons explaining employees' IS security behavior

The interviews revealed several culture-independent reasons for employees' IS security behavior. Specifically, employees' IS security behavior – across cultures – is learned from their previous work experience, morals and upbringing, work environment, professional identity, media, and social conformity. In addition, changing employees' IS security behavior is expected to require active organizational IS security communications in all countries.

Work experience: Employees' work experience may create false confidence concerning their IS security competence and, hence, preclude their interest in learning new IS security knowledge. In all four countries, employees with more work experience *believed* they followed secure working practices. The influence of work experience on an employee's IS security behavior was seen exclusively as positive by the respondents. Consequently, employees did not recognize that previous experiences could also hinder learning new and better IS security practices.

In addition, the interviews showed that employees had a tendency to consider all work experience equal from the viewpoint of one's IS security behavior. Typically, employees followed IS security procedures they had adopted during their previous jobs. The interviewees seemed to expect that different organizations have similar IS security, as the following observation from an employee from the UAE points out:

"...I had some experience in a previous company and the company before that also. I have been working in this industry for the past nine or ten years, so of course I have enough [security compliance-related] skills."

Morals and upbringing: The role of an employee's moral characteristics plays a key role in explaining his compliance and non-compliance with an organization's IS security policies. Hence, according to the respondents, a loyal, honest, and trustworthy person was assumed to comply with his or her employer's IS security policies and instructions. In contrast, non-compliance with the IS security procedure for personal benefit or harm to the employer was attributed to individual dishonesty, which was also linked to poor upbringing. Interestingly, some interviewees also linked non-compliance to the political climate in the workplace, where individuals may engender negative feelings about colleagues, and thereby fail to uphold the highest ethical standards.

Work environment: The interviews showed that employees' considerations regarding IS security threats in their working environment influence their IS security behavior. The interviewees expressed that IS security procedures, such as locking computers or selecting strong passwords, are pointless due to the strong physical and technical security in their working environment. As an example, employees expected that information security is taken care of by the IT department through technical safeguards, such as firewalls and malware protection. Consequently, the employees did not see personal effort as necessary. As another example, some of the interviewees trusted their colleagues. Thus, they believed that strict IS security instructions for the workplace were unnecessary, a perception illustrated by the following statement of a Chinese officer:

"They don't lock the PC; they lock the door so I think everything is safe… And also they trust others; they trust the system security…safeguard of company."

Professional identity: Employees' IS security behavior seemed to be intricately related to employees' professional identity; i.e., employees saw IS security as an integral part of their work responsibility. Professional identity was found to be associated with individual employees, as well as with working teams, business units, or even the entire company. For example, employees in human resources (HR) departments emphasized that IS security is an important aspect of their profession, as illustrated by a Swiss HR employee officer:

"I think in Human Resources you deal with so much sensitive information that it's clear that you have to be very careful of what you are telling to other people and so on. And if you, I don't know, have another profession..... [this may not be the case]..... If you are a carpenter, then that is no issue at all."

Media: The visibility of information security in the media has an impact on employees' IS security behavior. The influence of media on employees' IS security behavior was mentioned especially by employees with a personal interest in computers and ICT. The respondents also brought up the possibility that increasing IS security requirements in employees' personal lives (e.g., Internet banking, social media) may make employees more open to IS security requirements in their workplace. The close engagement of employees with media that were perceived to be susceptible to security concerns made the employees likely to comply with security policies, as described by a Swiss engineer:

"Since I'm studying and surfing the Internet, reading a lot of stuff and some kind of computer addict, so I think you learn it by yourself, if, just if you think about that. And also, I think also when it started with Internet banking; you're really starting to be aware."

Social conformity: Employees' IS security behavior was seen to be influenced by one's assumptions about others' IS security behavior. As an example, if an employee perceived that his or her co-workers were using a particular IS security safeguard, the employee tended to conform to this behavior. Such social conformity makes employees consciously or unconsciously behave according to the common rules of their work community. In addition, actively communicated norms seemed to have a stronger effect on compliance. The influence of social conformity on employees' IS security conventions is illustrated by a Swiss officer:

"*The people or the humans are not only individuals. They are living in a group. And if the majority of the group is doing certain things, then the others will follow.*"

Active communication: Active communication was seen as a key means in all countries for improving employees' IS security behavior. In this case, communications cover the following: a) the company's IS security policies, instructions, and other written information; b) IS security training; and c) active promotion of information security-related procedures by management. This was true across the different cultures studied. Some of these expectations were highlighted by a Swiss employee:

"It [IS security] is everyone's task. First of all, it's highest [priority] at the management level… who first have to promote information security issues. And then they have to also provide information to employees about the importance of information security."

4.2 Culture-dependent reasons that explain employees' IS security behavior

Employees' preferences regarding the means for learning IS security behavior vary across national cultures. The interviews revealed that employees in different countries prefer to learn IS security behavior by different means. In this study, employees' learning (i.e., developing new or changing old) of IS security behavior is analyzed using the following four learning paradigms: behaviorism, cognitivism, constructivism, and social constructivism. The different roles of behavioristic learning principles in different countries (i.e., one-way delivery of information, authority, learning through imitation and observation, punishments, rewards, and monitoring) were especially highlighted by the results.

Behaviorist learning methods: One-way delivery of information from management to employees was preferred in China. In the context of IS security, such behavioristic training implies that a teacher presents IS security issues by one-way communication from the trainer to the trainees, without necessarily customizing the training program to the trainees' learning processes, problem-solving styles (cognitivism), or individual or communal reflection of experiences (constructivism and social constructivism).

Employees' preference for behavioristic learning methods in China was highlighted by a Chinese employee as follows:

"I think discussions are not the most efficient. I think, maybe for us, a presentation is enough."

Authority: Our interviews suggest that employees' IS security behavior is influenced by authority, particularly in China and the UAE. For example, employees tend to comply with certain IS security policies and instructions if the employees are mandated to do so by a person in authority, such as their director or manager. Interestingly, some of the respondents felt free not to comply with the policies because authority figures had not explicitly signaled the importance of compliance, as described below by a Chinese manager:

"I do not do it (lock the computer) here, because managers don't ask me to do that…The manager should ask their subordinates to follow every type of company rule."

While employees of other countries expected management to play a more active role in promoting IS security, for Finnish employees, the active role of management in encouraging compliance with security policies had a smaller role in employees' compliance. Instead, Finnish respondents emphasized the personal responsibility of each individual employee to protect valuable information.

Imitation and observation: Another behavioristic learning method preferred in China, the UAE, and Switzerland—but not in Finland—was learning from the IS security behavior of management. The behavioristic learning paradigm assumes that people learn through imitation or observation. The interviews pointed out that employees in China, the UAE, and Switzerland perceived that the actions of management have a strong impact on their IS security behavior. A Chinese employee observed the following:

"I think we trust them. And if they said, it's right, I think, yeah, it's right."

Similarly, a UAE-based employee argued,

"Yeah, management's role is also important… We understand our duties, everything. This is because of the management. Because management influences us all."

Punishments, rewards, and monitoring: Another behavioristic learning method for IS security behavior emphasized during the interviews was the use of punishments and rewards. Punishments and rewards were considered effective in China, the UAE, but not in Switzerland or in Finland. The efficient use of punishments and rewards requires constant monitoring of employees' IS security behavior to allow instant rewarding and censuring. Most of the Asian employees in China and the UAE considered employer monitoring of employees an acceptable and effective method to impact employees' IS security behavior. However, in Switzerland and Finland, the interviewees considered employer monitoring of employees not only inefficient, but also inappropriate. In addition, Swiss and Finnish employees considered monitoring to have a negative effect on employees' IS security behavior, as it made employees feel that they were not trusted by their employer.

Cognitivist learning methods: Instead of one-way delivery of knowledge, imitation, and reinforcement in learning, cognitivism focuses on the mental activities of the learner and efficient processing of knowledge. Examples of cognitivism include using real-world examples of relevant assets, threats, and IS security accidents, and asking questions during the IS security training. Cultural differences were not observed in the interviewees' ideas about the benefits of such methods; principles of cognitive learning emerged across cultures.

Constructivist and social constructivist learning methods: While behaviorism and cognitivism are mainly directed by the external environment (e.g., organizational control, trainer), constructivism stresses the active role of the learner in constructing new knowledge either individually or in collaboration with other people. In particular, the Swiss interviewees indicated their preference for (and effectiveness of) constructive and social constructive teaching and learning methods over behavioristic learning methods. This is well illustrated by a Swiss employee here:

"Perhaps it (IS security) can also be discussed with the employees themselves. So that they are involved in the discussion. So that there's a better understanding… And so that they follow [IS security policies and instructions] better later on... ... So that they feel that they are just involved and that they can bring in their opinion. It's always better if you are involved in the discussion and in the decision..."

5 DISCUSSION

The key contribution of our study is the explanation of how different paradigms of learning are effective in the different cultures of Finland, Switzerland, the UAE, and China in changing employees' IS security behavior. Next, we discuss the four contributions in more detail.

First, the interviews revealed that employees in different countries prefer different means for learning IS security behaviors. These culture-dependent reasons explain employees' IS security behavior and mean that different learning paradigms—behaviorism, constructivism, or social constructivism—seem to work in different countries. In particular, behavioristic learning methods are preferred in China. In Switzerland, constructive and social constructive learning methods are preferred. To our knowledge, this is a new finding in the IS security literature, and suggests that previous models and methods focused on changing employees' IS security behavior may be limited to certain countries.

Second, inappropriately influencing employees' IS security behavior may have a negative effect on work motivation, such as lack of trust, an observation highlighted by Swiss and Finnish employees; Sanctions (Deterrence theory) is a case in point. In IS security literature, the role of sanctions in terms of deterrence theory has been strong (D'Arcy et al. 2008; Herath & Rao 2009a; 2009b; Li et al. 2010; Myyry et al. 2009; Siponen & Vance 2010). To our knowledge, this is a new finding in the IS security literature, and suggests new directions for future research.

Third, besides culture-dependent reasons, we found a number of culture-independent reasons, meaning that information security behavior across cultures is learned through previous work experience, morals and upbringing, work environment, professional identity, media, and social

conformity. In addition, in order to achieve a balance between employees' IS security behavior and organizational policies, initiatives and communications are expected from management across cultures. This finding provides important insights about the issues that need to be emphasized in the IS security interventions across cultures.

Fourth, our results suggest changing employees' IS security behavior using multiple means. This means there is no single "silver bullet" for improving employees' IS security behavior, but different means ranging from a management role model to influence of authority, relevance of the threat to the critical assets, and visibility of information security. Employees' IS security behavior is a complex phenomenon explained by various reasons, which is why different theoretical models find support in IS security research. They all have a role in explaining the complex phenomenon of employee compliance with IS security procedures. Given the complexity of the phenomenon, one interpretation of our results is that a reductionist method of finding a simple (parsimony) model with a few dependent variables may be difficult. Rather than using parsimony and generalizability as leading ideas behind the IS security research, future research should look for IS security context-specific theories, accuracy, and qualitatively rich descriptions (cf., Weick 1979). Example of these include IS security-specific theory development, in-depth qualitative research, and experiments that help to reveal the specific details of the phenomenon (accuracy).

5.1 Implications for Practice and Research

We would like to highlight the following implications for research and practice based on our findings.

First, given that employees in different countries prefer to learn IS security behavior by different means, IS security interventions need to be customized for each country. Our findings imply that behaviorist learning methods, such as one-way training or campaigning without customizing the training program to the trainees' learning processes, are effective in China. In turn, in Switzerland, constructive and social constructive teaching and learning methods should be used rather than behavioristic learning methods. In each country, employees' misconception that they already know appropriate IS security behavior may lead them to overestimate their IS security skills and compliance with organizations' IS security procedures. This creates a challenge to motivate experienced employees to acquire further skills on IS security.

Second, punishments and rewards (as behavioristic learning methods) can be used in China and the UAE, but their use must be carefully considered in Switzerland and in Finland. In addition, monitoring should be carefully considered in Switzerland and in Finland.

Third, in China, Switzerland, and the UAE, management must actively promote IS security. In Finland, each employee's personal responsibility for protecting valuable information needs to be emphasized.

Fourth, companies need to customize their IS security instructions and interventions to adapt to the cultural and local needs. This is especially relevant for global companies in which IS security management and policies may be centralized. Although high-level IS security strategies and policies are centralized and universal within a global company, lower-level IS security instructions should be customized. In addition, international standards (e.g., ISO/IEC 27001) and respective auditors should take into account the cultural differences pointed out in our study.

Since the interviews revealed that employees in different countries prefer to use different means for learning IS security behaviors, future research should take into account the possibility that different learning methods work differently in different countries. In addition, future research should further examine which learning paradigms—behaviorism, cognitivism, constructivism, or social constructivism—are most effective across different cultures. In addition, future research should further investigate what cultural characteristics lead to the different behaviors. Qualitative and quantitative research approaches could be used to study this issue.

Second, since the negative implication of sanctions was highlighted by Swiss and Finnish employees, future research should study the negative implications of sanctions. For example, future research

could design an experiment in which the effects of different sanctions on employees' attitude and trust towards their employer and IS security behavior are examined.

5.2 Limitations of the Study

The findings of this study are subject to the typical limitations of qualitative interview studies (see Lee & Baskerville 2003; Seddon & Scheepers 2012). Although the number of interviews is low from the perspective of statistical surveys, the key issue in interview studies is the point of saturation—not a high sample size or a certain predefined number of interviews (Seale 1999). In this study, the interviews were stopped when saturation was achieved. The literature suggests that the saturation point is different for different contexts; therefore, the number of interviews cannot be predefined. For example, Sarker et al. (2006) interviewed eight people, while Holmström Olsson et al. (2008) interviewed 22, and Sarker and Sarker (2009) conducted 25 interviews.

6 CONCLUSIONS

Employees' lack of adherence to IS security policies is a key problem for organizations. Previous studies have proposed different means aimed at explaining employees' compliance, such as the use of sanctions and monitoring (deterrence theory), and fear appeal and training, which represent different paradigms of learning (behaviorism, cognitivism, constructivism, and social constructivism). While these studies have increased our understanding of employees' IS security behavior, they do not test the validity of their models or methods across different cultural settings. Reflection on cultural studies suggests that cultural settings may influence the learning preferences and, hence, determine which means—behaviorism, cognitivism, constructivism, and social constructionism—are effective in different countries. Previous research on IS security behavior has not addressed this issue. Based on interviews in Finland, Switzerland, the UAE, and China, we argue that that while information security behaviors are learned, different paradigms of learning are effective in different cultures. Our results suggest that behavioristic methods are preferred in China, while constructivist methods are preferred in Switzerland. What is even more important is that providing non-preferred IS security interventions (e.g., monitoring or sanctions in Switzerland) seems to be negative in terms of improving information security.

These papers have implications for IS security research, editors and reviewers, and practitioners. For research, this study suggests the need to test the effect of different IS security interventions in terms of different learning paradigms in different countries. The implication for journal editors and reviewers is that they need to re-consider their reviewing policy; namely, they should accept papers that also show the limits of their model (not positive results) in some countries, in addition to positive results in different countries. Indeed, our results suggest that different cultures require different IS security interventions, and that decentralized IS security procedures should be customized to each country.

References

Albrechtsen, E. (2007). A qualitative study of user's view on information security. Computers & Security, 26 (4), 276-289.

Albrechtsen, E. and Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29 (4), 432-445.

Bandura, A. (1977). Social Learning Theory. General Learning Press, New York.

Beautement, A., Sasse, M.A. and Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. New Security Paradigm Workshop. In Proceedings of the 2008 Workshop on New Security Paradigms, p. 47-58, ACM, New York USA.

Bulgurcy, B., Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34 (3), 523-548.

Burchell, S., Clubb, C., Hopwoo, A.G., Hughes, J. and Nahapiet, J. (1980). The roles of accounting in organizations and society. Accounting, Organizations, and Society, 5 (1), 5-27.
Chan, M., Woon, I. and Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy & Security, 1 (3), 18-41.
D'arcy, J. and Hovav, A. (2007). Deterring internal information systems misuse. Communications of the ACM, 50 (10), 113-117.
D'arcy, J., Hovav, A. and Galletta, D.F. (2008). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20 (1), 79-98.
Delong, D.W. and Fahey, L. (2000). Diagnosing cultural barriers to knowledge management. Academy of Management Executive, 14 (4), 113-127.
Dinev, T., Goo, J., Hu, Q. and Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. Information Systems Journal, 19 (4), 391-412.
Greitzer, F.I., Kucher, O.A. and Huston, K. (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. Journal of Educational Resources in Computing, 7 (3), 1-16.
Herath, T. and Rao, H.R. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18 (2), 106–125.
Herath, T. and Rao, H.R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. Decision Support Systems, 47 (2), 154-165.
Holmström Olsson, H., Conchúir, E., Ågerfalk, P. and Fitzgerald, B. (2008). Two-stage offshoring: An investigation of the Irish bridge. MIS Quarterly, 32 (2), 257-279.
Hofstede, G. (2001). Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations. Thousand Oaks, CA.
Hofstede, G. (1998). Identifying organizational subcultures: An empirical approach. Journal of Management Studies, 35 (1), 1-12.
Hofstede, G. (1993). Cultural constraints in management theories. Academy of Management Executive, 7 (1), 81-94.
Hofstede, G. (1991). Cultures and Organizations: Software of the Mind. McGraw-Hill, London.
Hovav, A. and D'arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management, 49 (2), 99-110.
Hung, D. (2001) Theories of learning and computer-mediated instructional technologies. Educational Media International, 38 (4), 281-287.
Johnston, A.C. and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34 (3), 549-566.
Karjalainen, M. and Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. Journal of the Association for Information Systems, 12 (8), 518-555.
Kroeber, A.L. Kluckhohn, C. and Untereiner, W. (1952). Culture: A Critical Review of Concepts and Definitions. Wintage Books, New York.
Lee, A.S. and Baskerville, R.L. (2003). Generalizing generalizability in information systems research. Information Systems Research, 14 (3), 221-243.
Lee, S.M., Lee, S.G. and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information Management, 41 (6), 707-718.
Leidner, D. and Keyworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. MIS Quarterly, 30 (2), 357-399.
Li, H., Zhang, J. and Sarathy, R. (2010). Understanding compliance with Internet use policy from the perspective of rational choice theory. Decision Support Systems, 48 (4), 635-645.
Mezirow, J. (1991). Transformative Dimensions of Adult Learning. Jossey-Bass, San Francisco.
Miller, J. (2007). The Holistic Curriculum. 2nd edition. OISE Press, Toronto.
Miller, J.P. and Seller, W. (1985). Curriculum. Perspectives and Practice. Longman Inc, White Plains, NY.

Myers, M. and Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and Organization, 17 (1), 2-26.
Myers, M.D. and Tan, F.B. (2002). Beyond models of national culture in information systems research. Journal of Global Information Management, 10 (1), 24-32.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18 (2), 126-139.
Pahnila, S., Siponen, M. and Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 156b - 156b.
Palincsar, A.S. (1998). Social constructivist perspectives on teaching and learning. Annual Review of Psychology, 49, 345-375.
Pavlou, P.A. and Fygenson, M. (2005). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. MIS Quarterly, 30 (1), 115-143.
Puhakainen, P. and Siponen, M. (2010). Improving employee's compliance through IS security training: An action research study. MIS Quarterly, 34 (4), 1-23.
Sarker, S. and Sarker, S. (2009). Exploring agility in distributed information systems development (ISD) teams: An interpretive study in an offshoring context. Information Systems Research, 20 (3), 440-461.
Sarker, S., Sarker, S. and Sidorova, A. (2006). Actor-networks and business process change failure: An interpretive case study. Journal of Management Information Systems, 23 (1), 51-86.
Sasse, A., Brostoff, S. and Weirich, D. (2001). Transforming the 'weakest link' human/computer interaction approach to usable and effective security. BT Technology Journal, 19 (3), 122-131.
Seale, C. (1999), Quality in qualitative research. Qualitative Inquiry, 5 (4), 465-478.
Seddon, P. and Scheepers, R. (2012). Towards the improved treatment of generalization of knowledge claims in IS research: Drawing general conclusions from samples. European Journal of Information Systems, 21 (1), 6-21.
Schein, E.H. (1985). How culture forms, develops and changes. In Gaining Control of the Corporate Culture. (Kilmann, R.H., Saxton, M.J., Serpa, R. and Associates Eds.), pp. 17-43, Jossey-Bass, San Francisco.
Schulze, U. and Avital, A. (2011). Designing interviews to generate rich data for information systems research. Information & Organization, 21 (1), 1-16.
Siponen, M.T., Pahnila, S. and Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007): New Approaches for Security, Privacy and Trust in Complex Environments (Venter, H., Eloff, M., Labuschagne, L., Eloff, J. and Von Solms, R. Eds.), p. 133-144, Sandton, South Africa.
Siponen, M., Pahnila, S. and Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. Innovations in Information Technology, 1-5.
Siponen, M. and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34 (1), 1-15.
Skinner, B.F. (1969). Contingencies of Reinforcement: A Theoretical Analysis. Prentice Hall, USA.
Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005). Analysis of end user security behaviours. Computers and Security, 24 (2), 124-133.
Stinger, E.T. (1999). Action Research. Second edition. Sage Publications, Thousand Oaks CA.
Straub, D., Loch, K., Evaristo, R., Karahanna. E., and Srite, M. (2002). Toward a theory-based measurement of culture. Journal of Global Information Management, 10 (1), 13-23.
Walsham, G. (2006). Doing interpretive research. European Journal of Information Systems, 15 (3), 320-330.
Walsham, G. (2002). Cross-cultural software production and use: A structurational analysis. MIS Quarterly, 26 (4), 359-380.
Weick, K.E. (1989). Theory construction as disciplined imagination. Academy of Management Review, 14 (4), 516-531.