Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

A Conceptual Model for Explaining Violations of the Information Security Policy (ISP): A Cross Cultural Perspective

Khaled A. Alshare
Emporia State University, kalshare@emporia.edu

Peggy L. Lane
Emporia State University, plane3@missouriwestern.edu

A CONCEPTUAL MODEL FOR EXPLAINING VIOLATIONS OF THE INFORMATION SECURITY POLICY (ISP): A CROSS CULTURAL PERSPECTIVE

Khaled A. Alshare
Emporia State University
kalshare@emporia.edu

Peggy L. Lane
Emporia State University
plane@emporia.edu

ABSTRACT

This paper is an attempt to develop a model that explores the factors that affect the frequency of violations of information security policies (ISPs). Additionally, it examines the moderating effect of cultural attributes on the frequency of ISP violations. Does national culture affect the way managers and employees perceive and practice ISPs? If we understand why ISPs are violated, perhaps we can deter future violations before they occur. We look at three groups of factors and the impact they have on the frequency of violations of ISPs. The factors examined are 1) the individual characteristics and capabilities of employees, 2) the information security policy (ISP) itself and 3) management issues. Finally, the study examines the moderating effect of Hofstede's cultural dimensions (uncertainty avoidance, individualism/collectivism, and power distance) on the proposed model.

Keywords

Culture, ISP Violations, Conceptual Model.

INTRODUCTION

Is implementing technical solutions for security enough for a company to limit their exposure to security risks? Research tells us the answer is a definitive no, but technical solutions do have a role to play in security. Whitman (2003) states that "we often overlook the human solutions and instead opt for technology solutions, when in fact the human factors must be addressed first, with technology assisting in the enforcement of desired human behaviors." Son and Rhee (2007) report that Mitnick and Simon (2002) state that people who interact with the information assets of an organization are "truly security's weakest link". Son and Rhee (2007) suggest that "an organization's employees constitute one of its most significant security risks." The 5th Annual Global State of Information Security report (Berinato, 2007) is based on a study conducted online from March 6, 2007 through May 4 , 2007 in which 7200 CEOs, CFOs, CIOs, CSOs, VPs and directors of IT and IS, and security and IT professionals from more than 100 countries responded. In this study, for the first time, employees beat out hackers as the most likely source of a security incident. In some ways, this doesn't make sense when we learn from the report how much companies have increased their security precautions. They have added processes (57 percent have an overall security strategy up from 37 percent three years ago), deployed technology (including firewalls, intrusion detection infrastructure and use of encryption), and increased the number of Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs) hired. In fact, "out of every IT dollar spent, 15 cents goes to security", but security isn't improving. What has improved is the ability to capture and report data on security breaches (Berinato, 2007). Son and Rhee (2007) suggest that more research needs to be conducted to advance our knowledge of how to effectively manage human functions to improve the security performance of an organization. Understanding why security breaches take place helps in preventing violations of ISPs.

There are two primary objectives of this study. The first one is to examine factors that influence employees to respect or violate ISPs. The second objective is to explore the moderating impact of cultural attributes on the relationship between these factors and the frequency of ISP violations. To achieve these objectives, this paper will focus on a few countries that represent a variety of cultural sets. With the diffusion of the Internet and increase in e-commerce and outsourcing practices around the globe, the results of the study will be of great value to management around the globe.

LITERATURE REVIEW AND FORMULATION OF HYPOTHESES

The Individual Characteristics and Capabilities Factor

The individual characteristics and capabilities factor combines employees' awareness of the security policy, the level of technical skills of the employee, how much employees feel they are trusted and their willingness to trust others, the

employees' sensitivity to and respect for privacy issues, their level of individual ethics, and their level of accountability or feeling of responsibility. Individual and situational characteristics do influence ethical behavior intentions (Banerjee, Cronan, and Jones, 1998). If employees are not aware of the security policy, do not understand what it means from a technical perspective, feel they are highly trusted, do not respect privacy issues, have low levels of individual ethics, and low levels of accountability, then they are more apt to violate the policy. Adopting the company's information security policy (ISP) begins with the employees' awareness of information security practices. Ryan (2007) suggests that "the absence of awareness from appropriate training channels yields insufficient outcomes." He reports that no study has yielded a consensus information security awareness measurement. He examines a measurement that contains technology perception of information security awareness, policy perception of information security awareness, and threat-context perception of information security awareness. He found that the three information security awareness factors had positive correlations with both personal innovativeness and computer self-efficacy. Results of a study conducted by Peslak (2007) establish that merely having read a code of ethics can improve ethical moral judgments in certain situations. We posit the following:

H_1: Awareness, education, and training programs are negatively correlated with the number of ISP violations.

However, awareness by itself is not enough to consistently lower the frequency of security breaches. In cases where employees may be aware of the policy, they may not have sufficient technical education to understand what the policy means. Training programs that increase both awareness of the ISP and further understanding of technology so that the ISP can be understood will decrease the frequency of ISP violations that occur. Training programs should include scenarios that include all aspects of the ISP such as what can happen if you download "free" software and examples of how downloading free software has compromised security at other companies. We posit the following:

H2: The level of technical skills of employees is negatively correlated with the number of ISP violations.

Beyond awareness and understanding of technology, individual characteristics of the level of trust, sensitivity to privacy, ethics, and accountability need to be taken into consideration. The more an individual trusts someone else the more likely they are to violate ISPs. Trust has been measured by whether or not an employee will disclose a password to a secure system. (Slay, 2003) She posits that when considering trust and its effect on information security, other factors including attitude to authority, attitude to age and youth, value of loyalty and previous working relationship, formality in relationship, and gender differences need to be taken into consideration. An employee may hold trust in higher regard than they do the ISP. If that is the case, they will ignore the policy and share their password with a co-worker. They will do this because they trust that co-worker. We posit the following:

H_3: Trust of employees is positively correlated with the number of ISP violations.

Privacy refers to the privacy of personal data and is generally referred to as information privacy. In this study we are interested in how sensitive an individual is to protecting information about themselves as well as the identity of others. In the Global State of Information Security report (Berinato, 2007), it is reported that 22 percent of all companies surveyed employ a Chief Privacy Officer (CPO). Sixty percent of survey respondents posted privacy policies internally, only 24 percent posted policies on their external websites, and only 28 percent audited their privacy standards through a third party. In An Introduction to Computer Security: The NIST Handbook (1995) a section is included entitled "Computer Security is Constrained by Societal Factors." Rules, laws, and regulations may cause security to be increased or decreased. They state that "security and workplace privacy can conflict." Governments may require the flow of certain information that others would consider an invasion of privacy. Another example is the idea that the use of retinal scanning can be seen as an invasion of privacy in some environments and cultures. Skinner, Han, and Chang (2006) present a three-level information privacy taxonomy for collaborative environments to assist researchers in defining and clarifying information privacy components. They suggest the three dimensions of computation view, content view, and structural view can be used to create better information privacy policies, practices, and privacy enhancing technologies. We posit the following:

H_4: The sensitivity to privacy of employees is negatively correlated with the number of ISP violations.

Individual ethics is another aspect to include when considering individual characteristics. In their study, Pierce and Henry (1996) conclude "that a formal company code of computer ethics has an impact on decision making; therefore, it is crucial to have and to communicate to all members of the organization a formal company code of ethics with provisions which address the use of computers and computer technology." The results of a study conducted by Peterson (2002) indicate that the interaction between computer guidelines and belief in universal moral rules (ethics) was significant. Business professionals with a high belief in ethics exhibited high ethical intentions regardless of the knowledge about or existence of an ISP. We posit the following:

H_5: The ethics of employees is negatively correlated with the number of ISP violations.

Accountability is another important factor that could influence employees' behavior. Accountability is not only the legal responsibility that comes with the job description, but also the moral responsibility. Rao and Ramachandran (2007) caution that the appointment of a CISO clearly centralizes responsibility for information security in the organization. If there is a CISO then employees may feel they are not responsible or accountable for security, instead they may feel the CISO is solely responsible and accountable. As part of the training and awareness that takes place in companies, employees are often required to sign an acknowledgement statement which states they have read and understand the ISP. Some companies will require this statement to be signed on an annual basis. In one author's experience, security was tested at the individual level in employee offices at night. Sitting at the computer of an employee, a member of the security team would try to login as the employee. They would try obvious passwords and look around the office including under the keyboard for anything written down that could be the password. If the employee passed the test, a small card would be placed on the keyboard congratulating the employee for passing the test. The employee would see the card the next morning and know they had been tested and that they had passed. These tests served as a reminder of how important security was to the company and that the employee shared in the responsibility of keeping the company secure. We posit the following:

H_6: The accountability (feeling of responsibility) regarding security of corporate assets is negatively correlated with the number of ISP violations.

The Policy Factor

The policy factor examines the information security policy (ISP) itself and includes the level of the severity of penalties, the level of impact the policy has on the work environment, and the scope and clarity of the rules in the ISP.

Level of severity of penalties – In a press release by PricewaterhouseCoopers (2007) about the 2007 Global State of Information Security report, it is stated that "most companies do not document the enforcement procedures in their ISPs. Less than one-third (31 percent) include enforcement mechanisms." If the level of severity of penalties is unknown, employees are less likely to take the policies seriously. We posit the following:

H_7: The severity of the penalty of violations of the ISP is negatively correlated with the number of ISP violations.

Impact on work environment – The impact of ISPs on the work environment influences the behavior of employees as suggested by the Technology Acceptance Model of Davis (1989). Using the variables tested by Davis (1989) to explain what causes people to accept or reject information technology, we use those same variables to explore what causes people to accept or reject an ISP. The two variables are perceived usefulness and perceived ease of use. Davis defines perceived usefulness as the degree to which a person believes that using a particular system (in our case, ISP) would enhance his or her job performance. Perceived ease of use refers to the degree to which a person belives that using a particular system (ISP) would be free of effort. If employees perceive the ISP to assist them or remove some steps to their tasks, they may be more likely to follow the ISP; whereas, if employees perceive the ISP to add more steps or work to their tasks, they may be more likely to violate the ISP. We posit the following:

H_8: The negative impact of the ISP on the work environment is positively correlated with the number of ISP violations.

Scope and clarity of the rules – Whitman, Townsend, and Hendrickson (1999) state that in their study it is apparent that many individuals felt that if an organization does not specifically forbid the use of its computer resources for non-organizational purposes, then such use should be permitted thus enforcing the idea of a need for a clearly defined ISP. Moreover, Moor (2001) suggests "new applications of computing technology require replacing policy vacuums with good policies supported by reasonable justifications." The study conducted by Peterson (2002) provides evidence that for business professionals with a low belief in ethics, the presence of a clear ISP had a positive effect on ethical intentions. Doherty & Fulford (2005) hypothesized that those organizations that have a policy with a broad scope are likely to have fewer security breaches in terms of both frequency and severity than those organization that do not. Based on the above arguments, we posit the following:

H_9: The scope (clarity of rules) of the ISP is negatively correlated with the number of ISP violations.

The Management Factor

The third factor examines the management issues of the level of management support for security, the enforcement level of policy penalties, and the expenditures on security resources including both technical and human resources.

Management Support-Top management must show support for information security or it will not be taken seriously throughout the company. One way support can be shown is to appoint a Chief Information Security Officer (CISO). Support beyond appointing a CISO is considered key to the success of an organization's security efforts (Posthumus and von Solms,

2004). As von Solms (2001) states, "Without this management support, information security managers fight a very difficult, and often losing battle." (p. 216). Whitman (2003b) states "If employees know that management does not care about security, no training class teaching the importance of security and imparting valuable skills can be truly effective." We posit the following:

H_{10}: Management support for security is negatively correlated with the number of ISP violations.

Enforcement Level of Penalties-"Having policy and being able to enforce it are totally different things." (David, 2002, p. 506). In a press release by PricewaterhouseCoopers (2007) about the 2007 Global State of Information Security report, it is stated that "most companies do not document the enforcement procedures in their ISPs. Only 29 percent include collection of security metrics." If employees are not aware of penalties or if stated penalties are not enforced, employees will not take the ISP as seriously as the company intends or desires. One of the respondents in a study conducted by Knapp, Marshall, Rainer, and Ford (2006) stated "Enforcement is without a doubt the most critical ISP issue. While an organization can include whatever it wants in its security policy, this content is next to useless unless it is enforced." We posit the following:

H_{11}: The enforcement of the ISP is negatively correlated with the number of ISP violations.

Expenditures on security-Rao and Ramachandran (2007) suggest the appointment of a CISO clearly centralizes responsibility for information security in the organization; however, appointment without authority and resources is not enough. They suggest that security leaders must be provided with sufficient authority and resources to accomplish security objectives. Expenditures may be required for both people and technology. Hiring additional employees may be necessary to implement the ISP, train users, and implement technology. Expenditures may be required on technology such as firewalls, encryption techniques, and virus protection software as well as special software to assist in automatically enforcing critical policy areas (David, 2002). Employees' perceptions of IS expenditures will influence their behavior of ISP violations. For example, an employee who is aware of the capability of the IS department with respect to technology and staff skills, would be more hesitant to violate the ISP. Therefore, we posit the following:

H_{12}: The expenditures on information security resources are negatively correlated with the number of ISP violations.

Figure 1 displays the proposed research model.

The Moderating Effect of the Culture Factor

The security issues become more challenging in a network economy due to the nature of such an environment. Additionally, the trends in globalization and outsourcing magnify the responsibilities of security managers. Moreover, the new generation of information systems applications, which primarily are Internet oriented, have complicated security management by making these systems more vulnerable to security breaches. These factors (network economy, outsourcing, globalization, and Internet applications) mandate exploring the culture effect on security management practices. For example, managers in a network economy deal with a greatly diversified environment with respect to IT infrastructure and human resources.

To address the culture impact, Hofstede's cultural dimensions will be used as moderators for the relationships identified in the proposed research model. Hofstede surveyed 50 different countries (Hofstede, 1980, Hofstede, 1997). He identified four dimensions that can be used to distinguish among different cultures: power distance, individualism, masculinity, and uncertainty avoidance. A fifth dimension (long-term orientation) was later added (Hofstede and Bond, 1988). Among these cultural dimensions, we contend that uncertainty avoidance, individualism/collectivism, and power distance have the most direct impact on the relationship between the factors and the violations of the ISP. In the following section, we discuss the moderating effect of culture, as measured by three of Hofestede's cultural dimensions on the proposed model as shown in Figure 2.

Uncertainty Avoidance

Uncertainty avoidance (UAI) is defined as "the extent to which the members of a culture feel threatened by uncertain or unknown situations" (Hofstede, 1997, p. 113). The core values of cultures that exhibit higher uncertainty avoidance do not seem to support initiatives for information technology (Fandy 2000; Straub et al. 1997), as compared to cultures with lower uncertainty avoidance values. Cultures with higher uncertainty avoidance represent stability, risk avoidance, resistance to change, and strict control systems (Hofstede 1984). Individuals with higher uncertainty avoidance may be less prone to be proactive in exploring new information technology usage (Fandy 2000). Individuals high in this dimension are anxious about the future and actively avoid risk by devising various means of control including religion, laws, social plans, and written and unwritten rules. Therefore, individuals in higher uncertainty avoidance cultures will seek protection by sticking to existing patterns of educational processes that are heavily dependent on printed-information sources (Fagan et al., 2004). Thus, for

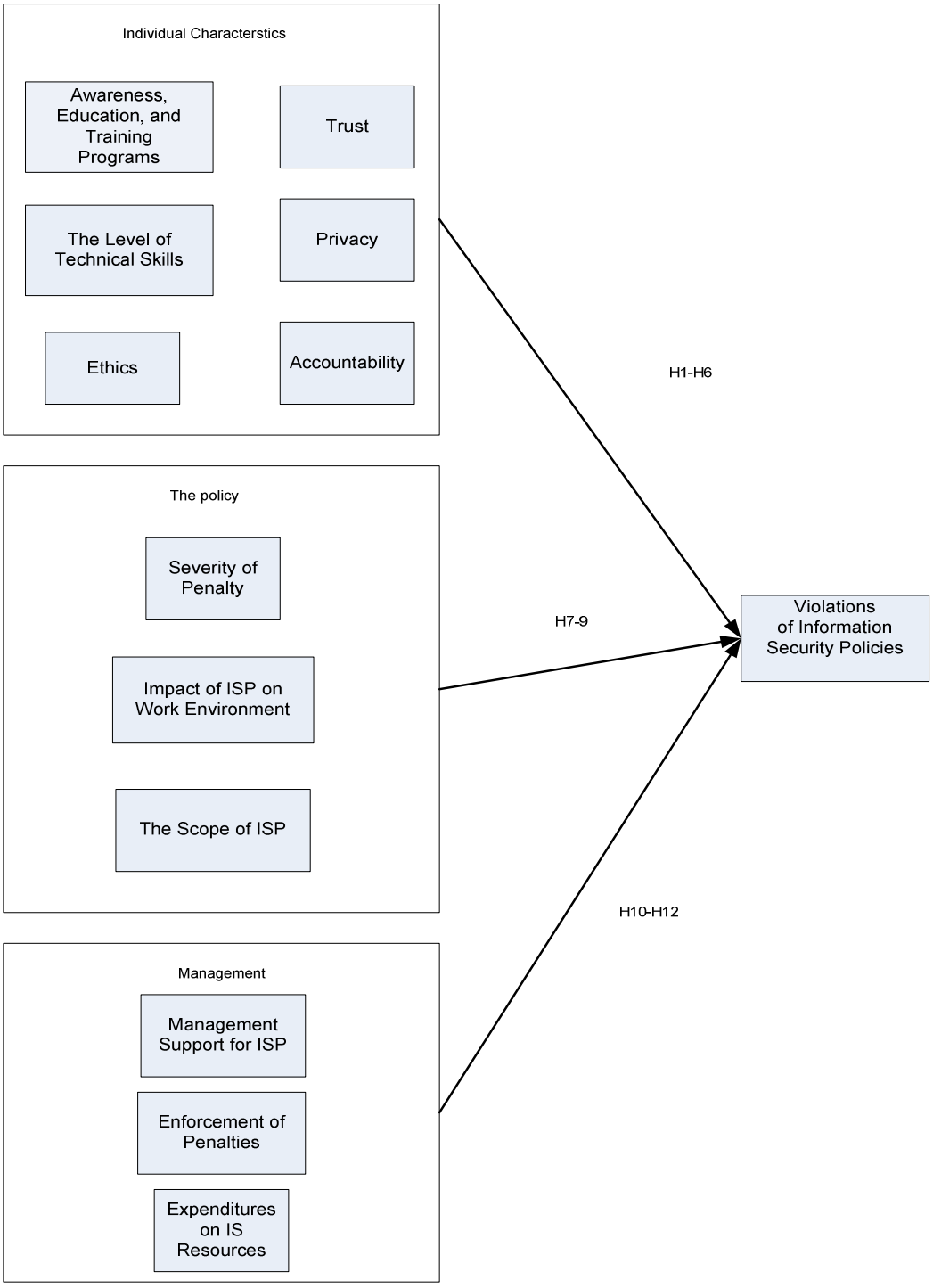

Figure 1: The Proposed Research Model

this group of individuals, educational and training programs represent the means of controlling and avoiding risks (e.g., violating the ISP).

In contrast, individuals with low uncertainty avoidance demonstrate risk-taking and tolerance to innovation and new ideas (Hofstede 1984). Additionally, they are more apt to try things by utilizing their technical skills and they are willing to take responsibility for their risky actions. By having more education and training programs related to IS, they will have more opportunities and ways to explore new technologies, and therefore; they are more subject to violating the ISP. We posit the following:

H_{1A}: Awareness, education, and training programs have a stronger positive (fewer violations) effect on violations of ISPs in cultures with high uncertainty avoidance.

H_{2A}: The level of technical skills has a stronger negative (more violations) effect on violations of ISPs in cultures with low uncertainty avoidance.

Individualism/Collectivism

Individualism (IDV) is defined as "the interest of the individual prevails over the interest of the group" (Hofstede, 1997, p. 50). Individualism refers to the relationship between the individual and the collectivity that prevails in a given society. Persons in a culture high in individualism have loose ties, and everyone is expected to look after his or her own personal interests (Hofstede 1980). The essential values of higher-individualism cultures emphasize autonomy, self-expression, independence, and performance-based reward achievement (Hofstede 1984, Akour et all 2006). As a result, they would be more cautious to have trust with people surrounding them such as their coworkers, more sensitive to privacy issues, more likely to make ethical decisions, and more receptive to accountability. Thus, these individuals are less likely to violate an ISP due to these characteristics.

On the other hand, low individualism or collectivist persons have close ties among members, hold group values and beliefs in high regard, and seek collective interests (Hofstede 1980). Collectivist cultures focus on the group as the dominant structure; thus, values such as conformity, coordination, and sacrifices are upheld (Hofstede 1997). As a result, they are more likely to share resources and accept responsibility as a group. Therefore, they have more confidence and trust in people surrounding them (e.g., coworkers) and they are less sensitive to privacy. Additionally, they perceive accountability as a group responsibility and thus, individual's mistakes are handled at the group level. Based on the above arguments, we posit:

H_{3A}: Trust has a stronger negative (more violations) effect on violations of ISPs in cultures with high collectivism.

H_{4A}: Privacy has a stronger positive (fewer violations) effect on violations of ISPs in cultures with high individualism.

H_{5A}: Ethics has a stronger negative (more violations) effect on violations of ISPs in cultures with high collectivism.

H_{6A}: Accountability has a stronger positive (fewer violations) effect on violations of ISPs in cultures with high individualism.

Power Distance

Power distance (PDI) is defined as "the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally" (Hofstede, 1997, p. 28). Individuals high in power distance accept power and wealth differences more readily than individuals low in power distance who value equality of classes and people. In a business environment, higher values of power distance mean considerable dependence of employees on their supervisors; employees are unlikely to approach and contradict their managers directly. In these cases, it is not unusual that an employee would provide or share information with others when the ISP prohibits sharing such information. Persons with low power distance demonstrate willingness to change and adjust to new work environments. Therefore, if the ISP dramatically impacts the work environment, then individuals with low power distance would adapt to new changes and not violate the ISP. Based on the above arguments, we posit:

H_{7A}: The severity of the penalty has a stronger positive (fewer violations) effect on violations of ISPs in cultures with high power distance.

H_{8A}: The impact of the ISP on the employees' work environment has a stronger positive (fewer violations) effect on violations of ISPs in cultures with low power distance.

H_{9A}: The scope of the policy (clarity of rules) has a stronger positive (fewer violations) effect on violations of ISPs in cultures with high power distance.

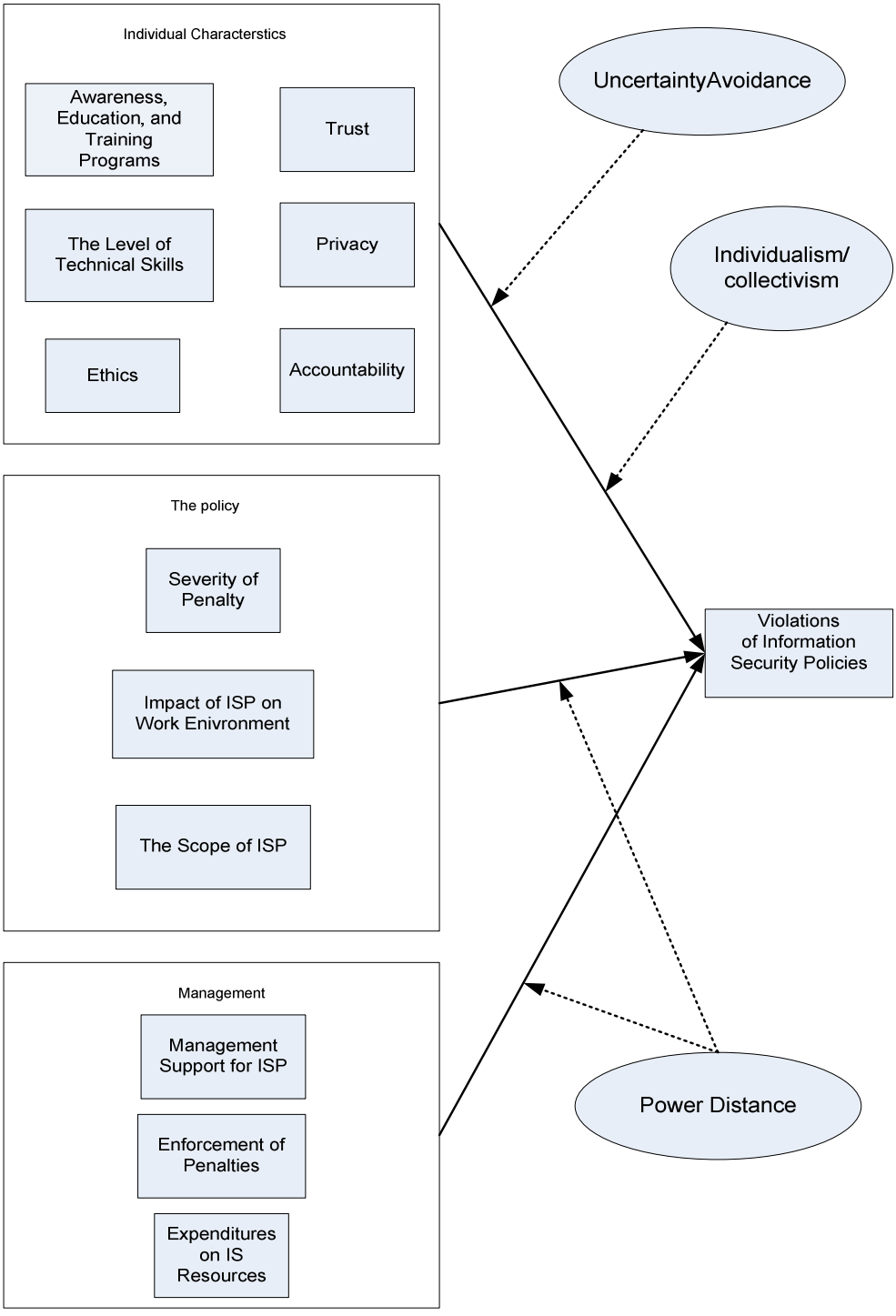

Figure 2: The Moderator Effect of Cultural Dimensions

H_{10A}: Management support has a stronger positive (fewer violations) effect on violations of ISPs in cultures with high power distance.

H_{11A}: Enforcement of penalties has a stronger positive (fewer violations) effect on violations of ISPs in cultures with high power distance.

H_{12A}: Expenditures on IS resources has a stronger positive (fewer violations) effect on violations of ISPs in cultures with high power distance.

RESEARCH METHOD

Instrument Development and Data Collection

An instrument based on the literature will be created to gather data on each of the variables. The instrument will be pilot tested and then administered to business professionals in a few select countries (e.g., USA, Mexico, and United Arab Emirates) that represent a variety of cultural sets.

Statistical Procedure

SPSS & LISREL software packages will be used to carry out the analysis. SPSS will be used to compute frequencies, means, standard deviation, reliability coefficients, and principle component analysis. A confirmatory factor analysis (CFA) approach will be taken with LISREL to validate the factor loadings identified in the principle component analysis. This validation will be conducted in the form of a measurement model consisting of all variables identified by the research model. A structural model will be then run testing the research model and hypotheses.

Measure of Constructs' Reliability and Validity

Reliability and validity of the measures will be assessed by following the steps conducted by King and Flor (2008).

1. Factor analysis will be performed on all items that measure the model constructs. Principle component analysis with varimax will be used.
2. Based on the initial factor analysis, constructs with eigenvalues greater than 1 will be retained.
3. Only items with loadings of at least 0.50 will be retained (Hair et al 2006).
4. Items with loadings greater than 0.50 on two or more constructs will be investigated thoroughly.
5. The above process will be repeated until we reached a stable measurement model.
6. The corrected item-total correlation will be computed for each item using only the items belonging to the same construct. The minimum acceptable value according to Hair et al (2006) is 0.5.
7. Cronbach's Alphas will be computed for each construct. An item will be dropped if the deletion of that item would significantly increase reliability. Generally, reliability coefficients of 0.70 or higher are considered acceptable (Nunnally, 1978).
8. A CFA using (Structural Equation Model) SEM will be performed on the final measurement model. LISREL will be used to carry out the analysis. Several goodness-of-fit indexes such as the Normed Fit Index (NFI), Non-Normed Fit Index (NNFI), Comparative Fit Index (CFI), and the Root Mean Square Error of Approximation (RMSEA) will be used to assess the validity of the constructs.

CONCLUSION

This paper is an attempt to develop a model that explores the factors that affect the frequency of violations of information security policies (ISPs). Additionally, it examines the moderating effect of cultural attributes on the frequency of ISP violations. The ability to determine what influences an employee to respect or violate the ISP will assist companies in planning training and communications about the ISP within their company. With the diffusion of the Internet and increase in e-commerce and outsourcing practices around the globe, the results of the study will be of great value to management around the globe.

REFERENCES

Akour, I., Alshare, K., Miller, M., and Dwairi, M. (2006) An exploratory analysis of culture, perceived ease of use, perceived usefulness, and Internet acceptance: The case of Jordan, *Journal of Internet Commerce*, 5, 3, 83-108.

Banerjee, D., Cronan, T., and Jones, T. (1998) Modeling IT ethics: A study in situational ethics, *MIS Quarterly*, 22, 1, 31-60.

Berinato, S. (2007) The 5th annual global state of information security - The end of innocence, *CIO Magazine*, August 28, 3-10.

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

Davis, F. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13, 3, 319-340.

Douherty, N. and Fulford, H. (2005) Do information security policies reduce the incidence of security breaches: An exploratory analysis, *Information Resources Management Journal*, 18, 4, 21-39.

Fagan, M., Neill, S., and Wooldridge, B. (2004) An empirical investigation into the relationship between computer self-efficacy, anxiety, experience, support and usage, *Journal of Computer Information Systems,* 44, 2, 95-104.

Hair, J., Black, W., Babin, B., Anderson, R., and Tatham, R. (2006) *Multivariate Data Analysis*. Prentice Hall. New Jersey.

Fandy, M. (2000) Information technology, trust, and social change in the Arab world, *The Middle East Journal,* 53, 3, 378-393.

Hofstede, G. (1997) *Cultures and Organizations. Software of the Mind. Intercultural Cooperation and its Importance for Survival.* New Jersey: McGraw-Hill.

Hofstede, G. (1984) The cultural relativity in the quality of life concept, *Academy of Management Review,* 9, 3, 389-398.

Hofstede, G. (1980) *Cultural Consequences: International Differences in work-related Values.* Beverly Hills, CA: Sage Publication.

Hofestede, G. and Bond, M. (1988) The Confucius connection: From cultural roots to economic growth, *Organizational Dynamics*, 16, Spring, 5-21.

King, W. and Flor, P. (2008) The development of global IT infrastructure, *Omega*, 36, 486-504.

Knapp, K., Marshall, T., Rainer, R., and Ford, F. (2006) Information security: Management's effect on culture and policy, *Information Management & Computer Security*, 14, 1, 24- 36.

Mitnick, K. and Simon, W. (2002) *The Art of Deception: Controlling the Human Element of Security*. Wiley, Indianapolis, IN.

Moor, J. (2001) The future of computer ethics: You ain't seen nothin' yet! *Ethics and Information Technology*, 3, 2, 89-91.

National Institute of Standards and Technology. (1995) An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. Downloaded on March 2, 2008 from http://csrc.nist.gov/publications/PubsTC.html

Nunnally, J. (1978) *Psychometric Theory.* McGraw-Hill, New York.

Peslak, A. (2007) A review of the impact of ACM code of conduct on information technology moral judgment and intent, *The Journal of Computer Information Systems*, 47, 3, 1-10.

Peterson, D. (2002) Computer ethics: the influence of guidelines and universal moral beliefs, *Information Technology & People*, 15, 4, 346-361.

Pierce, M. and Henry, J. (1996) Computer ethics: The role of personal, informal, and formal codes, *Journal of Business Ethics*, 15, 4, 425-437.

Posthumus, S. and von Solms, R. (2004) A framework for the governance of information security, *Computers and Security*, 23,8, 638-646.

PricewaterhouseCoopers (2007) press release dated September 10 and posted online. Downloaded November 8, 2007 from http://www.primenewswire.com/newsroom/news.html?d=126319.

Rao, S. and Ramachandran, S. (2007) Information security governance arrangements: The devil is in the details, *Proceedings of the Americas Conference on Information Systems,* August 9-12*,* Keystone, Colorado.

Ryan, J. (2007) Information security awareness: An evaluation among business students with regard to computer self-efficacy and personal innovation, *Proceedings of the Americas Conference on Information Systems,* August 9-12*,* Keystone, Colorado.

Skinner, G., Han, S., and Chang, E. (2006) An information privacy taxonomy for collaborative environments, *Information Management & Computer Security*, 14, 4, 382-394.

Slay, J. (2003) IS security, trust and culture: a theoretical framework for managing IS security in multicultural settings, *Campus-Wide Information Systems*, 20, 3, 98-104.

Son, J. and Rhee H. (2007) Out of fear or desire: Why do employees follow information systems security policies? *Proceedings of the Americas Conference on Information Systems,* August 9-12*,* Keystone, Colorado.

Straub, D., Keil., M., and Bernner, W. (1997) Testing the technology acceptance model across cultures: A three country study, *Information and Management*, 33, 1, 1-11.

von Solms, B. (2001) Information security – A multidimensional discipline. *Computers and Security*, 20, 6, 504-508.

Whitman, M. (2003) Enemy at the gate: Threats to information security, *Association for Computing Machinery. Communications of the ACM*, 46, 8, 91-95.

Whitman, M. (2003b) The human firewall - Leveraging your people to safeguard information resources, *Presentation at the First Annual Symposium on Information Systems Risk, Security & Assurance*, February 28, University of Akron, OH.

Whitman, M., Townsend, A., and Hendrickson, A. (1999) Cross-national differences in computer-use ethics: A nine-country study, *Journal of International Business Studies*, 30, 4, 673-687.