Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2011 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2011

A CROSS-CULTURAL STUDY OF THE EFFECTS OF STEA PROGRAMS AND TASK CHARACTERISTICS ON EMPLOYEES' BEHAVIOR TOWARD INFORMATION SYSTEM SECURITY POLICY COMPLIANCE

Xue Yang
Nanjing University, yangxue@nju.edu.cn

Wei Thoo Yue
City University of Hong Kong, wei.t.yue@cityu.edu.hk

Choon Lin Sia
City University of Hong Kong, iscl@cityu.edu.hk

A CROSS-CULTURAL STUDY OF THE EFFECTS OF STEA PROGRAMS AND TASK CHARACTERISTICS ON EMPLOYEES' BEHAVIOR TOWARD INFORMATION SYSTEM SECURITY POLICY COMPLIANCE

Yang, Xue, Nanjing University, Anzhong Building, Hankou Road 22, Nanjing, P. R. China, yangxue@nju.edu.cn

Yue, Wei Thoo, City University of Hong Kong, P7818, Academic Building, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, Wei.T.Yue@cityu.edu.hk

Sia, Choon Lin, City University of Hong Kong, P7811, Academic Building, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, iscl@cityu.edu.hk

Abstract

IS security policy is one of the essential tools to ensure the secure use of information systems and technological assets. To enhance the effectiveness of policy implementation, organizations rely on security training, education and awareness (STEA) program to help employees understand the IS security issues in the organization (informativeness) and encourage secure usage behaviors in line with security policies (persuasiveness). However, different levels of STEA informativeness and persuasiveness may have conflicting effects on employees' compliance behavior as greater informativeness could decrease the cost of non-compliance behaviors. In addition, urgency of a task may also lead employees to abandon the compliance behavior occasionally. A controlled lab experiment will be conducted to examine the phenomenon and test the hypotheses. We further add a cultural dimension to compare the compliance behaviors among employees in the United Kingdom, Hong Kong and mainland China. The results of this study can inform and guide researchers and practitioners to better enforce the IS security policy through better implementation of STEA programs.

Keywords: Security Training, Education and Awareness, Informativeness, Persuasiveness.

1 INTRODUCTION

As the use of information systems (ISs) becomes essential in supporting business activities, protecting the safety of corporate informational assets has become a critical challenge to many organizations. The challenge is great because many of the usage violations are carried out by internal employees (Gordon et al., 2006; Warkentin and Willison, 2009) who have the privilege to access some of the most sensitive information of the organization (Shaw et al., 1998), and such security breach behaviors can lead to direct negative impacts including corporate liability, loss of credibility and monetary damage (Cavusoglu et al. 2004). While organizations continue to provide improved technology-based solutions to eliminate IS security risks (Ernst and Young 2008; PricewaterhouseCoopers 2008), they also continuously improve the design of information security policies (ISPs) to prevent, detect and react to employees' unauthorized usage (Stoneburner et al., 2002) of information systems to achieve work-related objectives (Whitman et al., 2001).

However, in an increasingly fast-paced and flexible workplace, the policy per se cannot guarantee employees' compliance behavior (Boss and Kirsch, 2007; Siponen et al., 2007). In many occasions, organizations need to trust and offer employees enough privilege to perform their tasks. Thus, there is a need to understand IS abuse problems from the behavioral aspect of users to add an additional layer of mechanisms to ensure best practices in IS usage. Previous literature often focus on the economic tradeoffs in applying controls to prevent breach of information systems (e.g. Yue and Cakanyildirim, 2007) and little attention has been directed to the understanding of the different manifestations of corporate ISP enforcement measures and the external working environment that would impact the ISP compliance decision of the employees. In this study, we aim to fill this research gap by studying the extent of compliance behaviours influenced by security training, education and awareness (STEA) programs and work-related tasks.

Organizations usually implement various STEA programs to improve ISP compliance behaviors and reduce IS misuse (D'Arcy et al. 2009). These programs deliver different levels of informativeness and persuasiveness in their IS security messages which may cause unexpected conflicting effects. In addition, employees may occasionally decide not to comply with ISPs when compliance creates inconvenience in work-related tasks (Hui and Hu, 2008). In this study we focus on the task urgency as we believe it will most directly influence IS users' compliance decision. It should also be noted that human behavior is often affected by cultural factors. The effects of a STEA program or its task characteristics on one society may not be the same on another. In particular, Hofstede's Cultural Value Dimensions (Hofstede, 2005) that have been widely used to examine the impact of cultural differences (Taras et al., 2010) will be applied in this study.

In general, this study exemplifies the first attempt to address the impacts of specific STEA programs characteristics and the work-related task urgency on employees' STEA compliance behavior, particularly in a cross-cultural setting. The present study distinguishes from previous research which only examined individuals' awareness of the security issues (probably as a result of STEA programs) (e.g. Bulgurcu et al., 2010) or the mere presence of STEA programs (e.g. D'Arcy et al., 2009). Incorporating the task characteristics and cultural differences in the study is also a unique attempt that has not been considered by previous research, thus contributing to a deeper understanding of the phenomenon.

2 THEORETICAL BACKGROUND

Although it has been found that many IS usage violations are linked with malicious intent, very often work-related factors could also induce the violations. In this study, we plan to study the task-induced circumstances under which an individual may engage in inappropriate IS usage that is deemed violating the organisational information security policy (ISP). It is assumed that employees performing their tasks with benign intent may be invoked by external factors that motivate them to circumvent or breach the IS usage policy.

IS related ethical issues are complex and have a direct impact on the organisation domain. It has long been recognised that resolving ethical quandaries can improve the operational efficiencies of an organization (Smith and Hasnas, 1999; Harrington, 1996). Extant literature has established identifying characteristics of people in ethical aspect can be an effective way to deter misuse of IS (Banerjee, Cronan and Jones, 1998). In particular, this study introduces STEA programs, task and cultural characteristics as critical factors in influencing corporate users' compliance behaviour to IS security policies.

2.1 The Security Training, Education and Awareness (STEA) Program

Organizations these days promote sound IS usage through various STEA programs to improve the policy awareness and operational knowledge of the employees. Typically, these programs can be designed to serve two functions: informative and persuasive. STEA programs that are informative provide employees with technical and procedural knowledge of best practises on IS usage. Technical knowledge provides an overall scope on how a breach of code of ethics are detected and the likelihood

of detection, whereas procedural knowledge is about code of ethics (Harrington, 1996). Programs that are persuasive tend to focus on encouraging appropriate IS usage behaviour by inducing changes in attitudes and the perceptions of social norms and behavioural control.

However, informative and persuasive STEA programs can be a double-edged sword in cultivating sound IS usage if they are not properly conducted. First, regarding the informativeness of STEA, this conjecture arises from the fact that knowledge is the prerequisite in preventing or executing IS abuse. On one hand, such practices could prepare employees to be more aware of the possible ways of security breach and their detrimental impacts (D'Arcy et al., 2009). On the other hand, traditionally excessive individual liberties (e.g. information accessibility) are deemed to be harmful to security protection (e.g. national security) (e.g. Sagar, 2009; Sarikakis, 2008; Strickland 2005). Thus, STEA practices offering security information which may not be obtained otherwise could alter an employees' perceived difficulty of unethical acts due to exposure to the weaknesses of ISs and its related usage policy, and could even elicit IS abuse behavior.

Second, the persuasiveness of STEA concerns the framing of security-related messages (e.g. Chang, 2010). It has depicted that the strength and directions of persuasive messages can lead to different recipient responses such as acceptance of rejection (Holler et al., 2008). Moreover, some research indicates that the sanction or threatening appeals may be more effective than normative appeals when receivers are generally behaving in a benign way (e.g. Hasseldine et al., 2007). In contrast, other researchers hold that friendly persuasion is positively related to individual compliance behavior (e.g. Chung and Trivedi, 2003).

Obviously, organizations should avoid fear-induced environment when it comes to IS usage as punishment may produce undesirable behavioral, attitudinal and affective effects on individuals. Therefore, organizations should balance the degree of informativeness and persuasiveness of their STEA programs to maximize the programs' positive impacts and minimize the negative impacts on employees' IS security policy compliance decisions.

2.2 Task Characteristics at Workplace

Though STEA has been touted to be the most effective and practical measure to deploy in corporate IS security protection practices (D'Arcy et al., 2009), users may still perform noncompliance behaviors mostly because of the cost of compliance, such as work impediment (Bulgurcu et al., 2010) when individuals are morally open to changes (e.g. choosing not to follow the security rules in certain situations) (Myyry et al., 2009). When employees are required to make a decision whether to follow an IS security policy or not, they care about the particular corporate task that is carried out at the time. In fact, since a task involving IS security compliance behaviors require additional time and effort as compared to the same task without any security policy in place, an employee may perceive the compliance behavior a barrier to productivity (Siponen and Vance, 2010; Warkentin et al., 2004) and may immediately lead to perceptible or actual negative consequences to the employee (Bulgurcu et al., 2010). In some cases, complying with security requirements may even conflict with the employee's primary tasks or be detrimental to an employee's daily job-related tasks and activities (Pahnila et al., 2007). However, if the task at hand is not urgent enough to elicit such negative reactions toward the IS security policy, an employee may have less difficulty in complying with it as little additional time and effort would be required in such a scenario. Hence, task characteristics, in specific its urgency, will also be an important factor in affecting an employee's IS security policy compliance decision.

Furthermore, previous research has not paid attention to the interaction effect between task and STEA characteristics which means different levels of tasks urgency may impact ISP compliance behavior jointly with different STEA messages, rather than purely separate impacts. For example, strong informative STEA messages may be more effective in inducing compliance behavior with less urgent tasks and strong persuasive STEA messages could better encourage compliance behavior for urgent tasks. This is because, for example, informativeness can enhance the security protection capability (D'Arcy et al. 2009) especially when employees have time to execute it and persuasiveness can deter noncompliance behavior in emergent situations for its emphasis on the negative impacts on the

employees (Holler et al. 2008). Therefore, this study will also be the first one to examine the interaction effects between the two individual variables.

2.3 The Cultural Influence on Compliance Behavior

Previous research in the information systems field has explored specific culture-related factors such as the uncertainty avoidance and power distance (Png et al. 2001; Straub 1994), monochromic vs. polychromic culture (Rose et al. 2003), collectivism vs. individualism (Hwang and Kim 2007; Lowry et al. 2010; Mirchandani and Lederer 2010), ethical vs. developmental culture (Ruppel and Harrington 2001), etc, which result in conflicts of cultural values in the literature (Leidner and Kayworth 2006). However, these investigations were fragmented in terms of the consistent theoretical underpinning.

Among these different perspectives of cultural dimensions, Hofstede's Cultural Value Dimensions have been widely applied to measure national culture characteristics in different fields (e.g., information systems research) for more than three decades (Ford et al. 2003; Taras et al. 2010; Wei et al. 2010; Yoon 2009). According to his framework for assessing culture (Hofstede and Hofstede, 2005), there are 5 cultural dimensions including 1) Power distance index (PDI) which measures the extent to which people expect and accept that power is distributed unequally; 2) Individualism (IDV) which refers to the extent to which people define themselves apart from their group memberships; 3) Masculinity (MAS) which describes the value placed on traditionally male or female values (as understood in most Western cultures). In a masculine culture, people value competitiveness, assertiveness, ambition, and the accumulation of wealth and material possessions, while in a feminine culture, people value relationships and the quality of life. Furthermore, the differences between gender roles in a masculine culture are more dramatic than in a feminine culture; 4) Uncertainty avoidance index (UAI) which describes how much people are anxious about the unknown, and as a consequence, they will attempt to cope with anxiety by minimizing uncertainty; and 5) Long term orientation (LTO) which refers to the importance attached to the future versus the past and present by a society. In long-term oriented societies, people value actions and attitudes that affect the future, while in short-term oriented societies, people value actions and attitudes that are affected by the past or the present.

A score analysis on cultural dimensions by Geert Hofstede[1] found that UK and Hong Kong cultures differ significantly in terms of PDI, IDV and LTO. Their scores for MAS and UAI are comparable. China and Hong Kong cultures are only significantly different in the dimension of UAI, yet Hong Kong culture has long been considered as an integration of both China and UK due to its historical relationship with UK. Thus, to highlight the effects of culture on the effectiveness of different types of STEA, we will focus on the PDI, IDV, LTO and UAI dimensions and examine their impacts on the these three countries/areas' corporate user compliance to security enforcement policies.

[1] http://www.geert-hofstede.com

3 RESEARCH MODEL AND HYPOTHESES

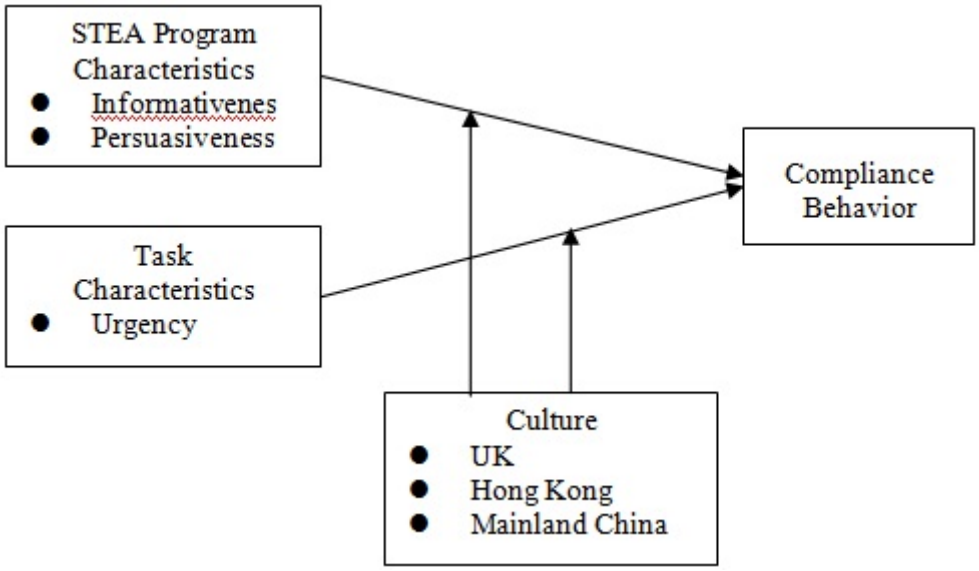

Fig. 1. Research Model

Our conceptual model is shown in Figure 1. First, since the extent to which informativeness and persuasiveness of a STEA messages perceived by an employee could either lead to unwillingness to comply with the IS security policy (i.e. a low level of informativeness and persuasiveness) or attempts to breach the IS security policy (i.e. a high level of informativeness and persuasiveness), we propose an inverted-U relationship between the informativeness and persuasiveness of a STEA message and an employee's compliance behavior. We argue that STEA messages that are designed to balance the degree of informativeness and persuasiveness can have the best enforcement effects.

Second, it is hypothesized that when employees are carrying out daily routines that are not expected to be completed immediately, it will be more likely for them to follow the detailed requirements of the IS security policy. However, if the task at hand is urgent or required to generate quick outputs, the IS security policy will become a hurdle in accomplishing the task in terms of time and effort. Hence, when a task is urgent, an employee is hypothesized to be more likely to break the policy which may lead to less compliance behavior.

Studies have shown that culture plays a significant role in the effectiveness of a message being delivered in a society (e.g. Gregory and Munch, 1997). In this study, we hypothesize that cultural difference will moderate the relationship between STEA messages or task characteristics and employees' compliance behaviour to the IS security policy. In particular, we base our hypotheses on the assumption that Hong Kong employees are more receptive to more informative and authoritative messages and are more likely to place urgent tasks a more important weight than IS security policy. Other individual factors such as the employee demographics including position, tenure or expertise level may also affect the decision making, thus will be included in the research model as control factors.

4 PROPOSED RESEARCH METHODOLOGY

Our study will use standard survey and lab experimental techniques to collect data from working professionals in different industries and organizations. Based on Geert Hofstede's cultural dimensions, we will recruit participants from the UK, Hong Kong and mainland China to participate in a lab experiment that requires the participants to complete decision tasks that reveal their true preferences for compliance, self interest and group interest. Data collected will allow us to understand the effects of culture on compliance behaviour. Similar to Kuo and Hsu (2001)'s study, we plan to manipulate the

STEA messages and the task characteristics to influence an employee's perceived behavioral control, and investigate how this may affect abusive IS usage behavior. Furthermore, we propose that cultural factors would intervene with the IS policy compliance decisions.

In the experiment, subjects will be asked to complete a number of simple tasks through a computer system. The task requires the use of a password that belongs to an information owner. At the beginning of the experiment, each subject will receive a STEA message and a set of instructions. The STEA message will be designed to reflect the different levels of informativeness and persuasiveness (e.g. Chung and Trivedi, 2003; Hasseldine et al., 2007; Kuo and Hsu 2001). In the instructions, the manager's password is provided "by accident". Some subjects will be required to finish the tasks as quickly as possible and they will be told that their payoff will be linked to how quickly they can finish their tasks or how many tasks they can complete in the lab. Other subjects will be allowed to finish the task without any time constraints. This kind of incentivized decision task helps ensure that subjects reveal their true preferences for compliance, self-interest and group interest through their decisions. Our research design will be reviewed internally by the ethics committees at the University of Nottingham and City University of Hong Kong. The research team will also address any data privacy concerns that the participants may have.

5 IMPLICATIONS AND CONCLUSION

This study represents one of the earliest attempts by researchers to empirically investigate how STEA programs can be designed to influence employees and how task characteristics may affect compliance behavior under different cultural settings. The results will benefit both academics and practitioners in several aspects.

The benefits to academic research in Information Systems include the conceptualization of STEA function into "informative" and "persuasive" and the incorporation of task characteristics and culture as a predictor of compliance behaviour. The classification of STEA function enables future researchers to address complex STEA related problems systematically. The inclusion of culture as a predictor of compliance highlights the importance of the social aspects of computer user behavior and the need to consider these aspects in future research models. The methodological contribution is demonstrated by the use of experimental economic techniques in studying the true preference and behaviour that may result in threat on information systems arising from trusted users.

Findings from this study will also have significant management implications to the design and implementation of STEA programs within an organization by considering the specific task characteristics. Specifically, security practitioners need to discern the potential conflicting effects of informativeness and persuasiveness in STEA programs by taking task urgency into account. Furthermore, an understanding of the effects of culture on information security behaviors is important to many multinational organizations, as well as organizations that need to manage employees from diverse cultural backgrounds.

To summarize, this study recognizes the impacts of different levels of informativeness and persuasiveness in STEA programs on employees' compliance behaviors and considers the importance of task urgency. Furthermore, a cultural dimension is added to compare the compliance behaviors between employees in Hong Kong, UK and mainland China. We propose a controlled lab experiment design to examine the phenomenon and test the hypotheses. The results of this study will be able to guide researchers and practitioners to better enforce the IS security policy.

Acknowledgements. The authors gratefully acknowledge a research grant from the City University of Hong Kong (SRG Project No. 7002527) in support for this study.

References

Boss, S. R. and Kirsch, L. J. (2007). The last line of defense: motivating employees to follow corporate security guidelines. In Proceedings of the 28th International Conference on Information Systems, Montreal, December 9-12.

Cavusoglu, H. Mishra, B. and Raghunathan, S. (2004). The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9 (1), 69-104.

Chang, C. C. (2010). Message framing and interpersonal orientation at cultural and individual levels involvement as a moderator. International Journal of Advertising, 29(5), 765-794.

D'Arcy, J. Hovav, A. and Galletta, D. (2009). User awareness of security counter-measures and its impact on information systems misuse: A deterrence approach. Information Systems Research, (20:1), 79-98.

Ernst & Young. (2008). Moving beyond compliance: Ernst & Young's 2008 global information security survey.

Gordon, L. A. Loeb, M. P. Lucyshyn, W. and Richardson, R. (2006). CSI/FBI computer crime and security survey. Computer Security Institute.

Gregory, G. D. and Munch, J. M. (1997). Cultural values in international advertising: An examination of familial norms and roles in Mexico. Psychology and Marketing, 14(2), 99-119.

Harrington, S. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS Quarterly, 20(3), 257-277.

Hasseldine, J. Hite, P. James, S. and Toumi, M. (2007). Persuasive communications: Tax compliance enforcement strategies for sole proprietors. Contemporary Accounting Research, 24(1), 171.

Hofstede, G. and Hofstede, G. J. (2005) Cultures and Organizations: Software of the Mind. 2nd Edition. New York: McGraw-Hill.

Hui, W. and Hu, P. (2008). Examining end-user information security policy compliance: An exploratory study. Proceedings of the Workshop on e-Business (WeB), Paris, France, 13 December 2008.

Kuo F. and Hsu, M. (2001). Development and validation of ethical computer self-efficacy measure: The case of softlifting. Journal of Business Ethics, 32, 299-315.

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 Hawaii International Conference on System Sciences, Los Alamitos, CA: IEEE Computer Society Press, pp. 156-166.

PricewaterhouseCoopers. (2008). Employee behaviour key to improving information security, new survey finds. June 23.

Sagar, R. (2009). Who holds the balance? A missing detail in the debate over balancing security and liberty. Polity, 41(2), 166-188.

Shaw, E. Ruby, K. and Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2-98, 1-10.

Siponen, M. T., and Vance, A. (2010). Neutralization: new insight into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.

Siponen, M. T., Pahnila, S., and Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. in New Approaches for Security, Privacy and Trust in Complex Environments, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Boston: Springer, pp. 133-144.

Stoneburner, G. Goguen, A. and Feringa, A. (2002). Risk management guide for information technology systems. NIST Special Publications 800-30, White Paper, United States Department of Commerce, Gaithersburg, MD.

Taras, V. Kirkman, B. L. and Steel, P. (2010). Examining the impact of culture's consequences: A three-decade, multilevel, meta-analytic review of Hofstede's cultural value dimensions (vol 95, pg 405, 2010). Journal of Applied Psychology, 95(5), 888-888.

Warkentin, M. and Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101-105.
Warkentin, M. Davis, K. and Bekkering, E. (2004). Introducing the check-off password system (cops): An advancement in user authentication methods and information security. Journal of Organizational and End User Computing, 16(3), 41-58.
Yue, W. and Çakanyildirim, M. (2007). Intrusion prevention in information systems: Reactive and proactive response. Journal of Management Information Systems, 24(1), 329-353.
Yue, W. Çakanyildirim, M. Ryu, Y. and Liu, D. (2007). Network externalities, layered protection and it security risk management. Decision Support Systems, 44 (1), 1-16.