

Influence of HRM Practices on Privacy Policy Compliance Intention: A Study among Bank Employees in Korea¹

Youngkeun Choi² and Taejong Yoo³

*Sangmyung University, 20, Hongjimun 2-gil, Jongno-gu, Seoul 110-743, Korea
penking1@smu.ac.kr*

Abstract

This research project investigates human resource management practices related to information privacy policy compliance by individuals in banks industry. The results of this survey of 257 bank employees in Korea indicate that certain human resource management practices within organizations (referred to as developmental-oriented appraisal, externally or internally equitable reward, selective staffing and training for career development) contribute to a social exchange process. This process is distinct from the formal compliance training procedures and is shown to influence employee perceptions of social exchange to engage in compliance activities, which contributes to behavioral intention to comply with information privacy policies. Implications for managers and researchers are discussed.

Keywords: *information security behavior; human resource management practices; social exchange theory; organizational commitment; privacy policy compliance intent*

1. Introduction

Most studies in information systems field has primarily focused on technical issues concerning the design and implementation of security subsystems (Choo, 2011; Zafar and Clark, 2009). These technical, externally focused efforts are important, but the individual user within an organization is critically important in properly securing information assets (Leach, 2003; Posey *et al.*, 2011; Sasse *et al.*, 2001; Stanton *et al.*, 2005; Vroom and von Solms, 2004; Warkentin and Willison, 2009).

Some of the study in this area includes computer security behaviors (Loch *et al.*, 1992; Stanton *et al.*, 2005); security behavior in the home setting (Anderson, 2005); access control and security perceptions (Zhang, 2005; Furnell *et al.*, 2007; Post and Kagan, 2007); and malicious behaviors or computer abuse in organizations (Straub and Nance, 1990; Lee *et al.*, 2004). However, the respondents in these studies are typically IT administrators or top-level managers (*e.g.*, Straub and Collins, 1990; Loch *et al.*, 1992; Knapp *et al.*, 2005; Ma and Pearson, 2005; Dhillon and Torkzadeh, 2006) rather than representatives from the end-user community. The fact that the respondents in prior studies were largely those responsible for setting up and running technical security initiatives raises the question of whether or not their views are likely to be representative of the organization as a whole (Finch *et al.*, 2003).

Recently, there has been some research on end-user policy compliance. In an empirical vein, D'Arcy and Hovav (2004) followed deterrence theory and developed a theoretical model that examines the effect of deterrent security countermeasures on the perceived certainty and severity of sanctions, which in turn, leads to IS misuse intentions whereas Straub (1990) finds that deterrence measures reduce computer abuse in organizations. Albrechtsen (2007) conducted a qualitative study of user views on information security

¹ This research was supported by a 2013 Research Grant from Sangmyung University

² First author

³ Corresponding author

and found that users do not perform many information security actions and that they prioritize other work tasks in front of information security. Albrechtsen (2007) argues that a main problem regarding user roles in information security work is their lack of motivation and knowledge regarding information security and related work. Post and Kagan's (2007) study also found that end-users perceived security practices to be a hindrance in their normal routine. In an evaluation of security policy compliance, Chan *et al.*, (2005) studied the security climate in organizations and found that management practices and coworker socialization have an impact on employee perceptions of the information security climate which, in addition to self-efficacy, positively impact security policy compliance behavior. Stanton *et al.*, (2003) examined the effect of organizational commitment on variety of security behaviors including security policy compliance. Pahlila *et al.*, (2007) found that employee attitudes, normative beliefs, and habits all have a significant effect on employee intentions to comply with IS security policy whereas threat appraisal and facilitating conditions have a significant impact on shaping attitudes towards compliance.

Although several researchers pay their attention to this issue, the investigation of policy compliance is still embryonic and poses many opportunities for empirical research. If then, is the human resource management (HRM) practices capable of supporting, enhancing or perhaps alternatively, diminishing the security policy compliance intention among employee. However, there is little existing insight into how organizational management, also called HRM practices, influence employee compliance outcomes. Moreover, when the compliance context concerns security policy compliance, the scope of empirical studies from which to inform current research becomes even narrower. Based on this gap in both the academic and the practitioner literature, the following research question is posed:

RQ: How do the HRM practices in organization influence employees' security policy compliance intentions?

This study aims to illuminate certain HRM practices associated with social exchange relationship and to clearly identify how these HRM practices influence the perceptual outcomes associated with security policy compliance. This study tests an application of social exchange theory in a unique context involving policy compliance intentions. Further, the results provide promising insights for managers who seek to development HRM practices in which compliance intent is elevated rather than weakened.

2. Theoretical Background and Hypothesis

2.1. Social Exchange Theory

In general, issues related to information security behaviors are follows: how security conscious behaviors are shaped or influenced, what motivates people to undertake security measures, what motivates people to carry out actions that are prescribed by organizations, *etc.*, these issues can be studied through the lens of theories borrowed from disciplines including psychology, sociology, and criminology that give us insights into behaviors, motivations, values, and norms. These studies lead us to understand that HRM practices are influential elements to an individual; however, this influence has not been examined in a security context, and their possibility to influence perceptions of compliance beliefs and intentions has not previously been established. Social exchange theory (Blau, 1964; Homans, 1961) provides a framework for understanding the relationship of HRM practices and compliance attitudes as it specifically relates to the outcomes of social exchange relationship to the organization and cognitive processes individuals experience as part of the exchange process.

Social exchange theory (Blau, 1964; Homans, 1961) explained the motivation behind the attitudes and behaviors exchanged between individuals. Eisenberger, *et al.*, (1986)

expanded this work by proposing and establishing that the theory of social exchange also explains aspects of the relationship between the organization and its employees. They noted that employees form general perceptions about the intentions and attitudes of the organization toward them from the policies and procedures enacted by individuals and agents of the organization, attributing human-like attributes to their employer on the basis of the treatment they receive (Levinson, 1965). In this way, employees see themselves as having a relationship with their employer that is parallel to the relationships individuals build with each other. Recognizing this tendency to personify the organization, they applied social exchange theory to the relationship between the personified organization and its employees. In particular, they predicted that the positive, beneficial actions directed at employees by the organization and/or its representatives contribute to the establishment of high-quality exchange relationships that create obligations for employees to reciprocate in positive, beneficial ways” (Settoon *et al.*, 1996).

By examining the antecedents of security policy compliance intent from the perspective of social exchange theory, a research model is formed that provides a unique framework for understanding the influence of HRM practices on individual compliance outcomes. The security compliance research model in this study suggests that HRM practices within organizations influence employees’ behavioral intentions to comply. The relationship between the effects of HRM practices on behavioral intent is purposeful and is positioned to remain consistent with the seminal works of Blau (1964) and Homans (1961) in articulating social exchange theory.

Based upon the theoretical framework described above, the following section provides support for the relationships and presents the hypotheses of the present study. The research model and its associated hypotheses are grounded in and supported by extant literature in social exchange theory and policy compliance.

2.2. Hypothesis Development

Ostroff and Bowen (2000) relied on social exchange theory in developing hypotheses about the relationships among HRM practices, attitudes, and performance. They proposed that human resource practices shape work force attitudes by molding employees’ perceptions of what the organization is like and influencing their expectations of the nature and depth of their relationship with the organization. Employee attitudes and behaviors (including performance) reflect their perceptions and expectations, reciprocating the treatment they receive from the organization. In their multilevel model linking HRM practices and employee reactions, they depicted relationships suggesting that HRM practices are significantly associated with employee perceptions and employee attitudes.

HRM practices can be classified as “control” or “commitment” practices (Arthur, 1994; Walton, 1985; Wood and de Menezes, 1998). Control approaches aim to increase efficiency and reduce direct labor costs and rely on strict work rules and procedures and base rewards on outputs (Arthur, 1994). Rules, sanctions, rewards, and monitoring regulate employee behavior (Wood and de Menezes, 1998). In contrast, commitment approaches aim to increase effectiveness and productivity and rely on conditions that encourage employees to identify with the goals of the organization and work hard to accomplish those goals (Arthur, 1994; Wood and de Menezes, 1998).

In the perspective of commitment approach, HRM practices have been considered to be effective tools for enhancing employees’ commitment to organization (Ulrich, 1997). Ogilvie (1986) perceives HRM practices as concrete, tangible programs designed to develop employees’ commitment to organization. They include selective staffing, developmental appraisal, competitive and equitable compensation, and comprehensive training and development activities (Ichniowski *et al.*, 1997; MacDuffie, 1995; Snell and Dean, 1992; Youndt *et al.*, 1996).

First, a lot of studies suggest that performance appraisal is significantly correlated to employees’ commitment to organization (Jaiswal, 1982; Ogilvie, 1986; Singh, 2000).

Paul and Anantharaman reveal that developmental-oriented appraisal show a significant positive relationship with employees' commitment to organization. Second, among various HRM practices, it has been found that rewards such as compensation and benefit have a greater influence on employees' commitment to organization (Angle, 1983; Mottaz, 1988; Mowday *et al.*, 1982; Steers and Spencer, 1977). Advanced compensation practices enable the organization to retain essential employees for longer periods of time (Lawler and Jenkins, 1992; Mobley, 1982). Profit sharing leads to better cooperation, better communication, and better participation (Weitzman and Kruse, 1990). Profit sharing and stock ownership encourage team members to identify with the organization and work hard on its behalf (Pfeffer, 1998). Third, some studies suggest that selective staffing influence employees' commitment to organization. For most IT professionals, a significant part of their motivation comes from the recognition they get from managers for doing an outstanding job (Agarwal and Ferratt, 1999; Gomolski, 2000). Jaiswal (1982) and Ogilvie (1986) found relationships between specific practices such as promotion policies and employees' commitment to organization. Finally, it has been found that training activities not only develop employees and improve their skills and abilities but also enhance their satisfaction with the job and their commitment to the organization (Harel and Tzafirir, 1999; Kalleberg and Moody, 1994; McEvoy, 1997). Laabs (1997) found that a training program at Bell Helicopter reduced employee turnover. Career development strengthens the psychological contract and motivates employees to have continued commitment to the firm (Harel and Tzafirir, 1999).

Security-related behaviors may be connected to his/her closeness to the organization as well as an individual's motivation to protect organizational information assets due to an awareness and fear of the outside environment. As such, relevant research stream that may shed light on positive organizational behaviors of policy compliance is employee commitment to organizational well-being. Social exchange theory posits that strong social bonds prevent a person from committing negative behaviors. Therefore, an employee's commitment to an organization is likely to play a role in his/her engagement in security behaviors. People in an organization are less likely to enact counterproductive computer behaviors that put the company systems at risk if they are highly committed to their organizations (Stanton *et al.*, 2003). In a security context, such employees tend to believe that they should do their security conscious behaviors which have an impact on the achievement of overall organizational information security. Thus, we can expect that:

Hypothesis 1 *Developmental-oriented appraisal system will positively affect employees' behavioral intent to follow security policies.*

Hypothesis 2 *Externally or internally equitable reward system will significantly affect employees' behavioral intent to follow security policies.*

Hypothesis 3 *Selective staffing system will positively affect employees' behavioral intent to follow security policies.*

Hypothesis 4 *Comprehensive training system will positively affect employees' behavioral intent to follow security policies.*

3. Methods

3.1. Data

When there are significant regulatory sanctions or legal liability, most organizations should ensure a high level of compliance with emerging privacy policies. To test our hypotheses, we sought an organizational environment in which privacy compliance is paramount. Due to the regulatory requirements imposed on customer information privacy protection, the bank industry can be an excellent test bed to investigate the research questions of this study.

The unit of analysis for this research project is the individual employee of a bank organization. Such individuals include nearly all staff (employees) of organizations that provide banking services to individuals (customers). They may include administrative staff members (managers, administrative assistants, and other non-banking personnel). For the survey, this study contacted three banks in Korea. A total of 300 bank employees responded to the survey, of which 257 responses were valid and usable for analysis. A total of 156 (61%) of the respondents were female, while 101 (40%) were between the ages of 26 and 39. Also, 47% of the respondents have been bank employees for at least 10 years.

3.2. Variables

The HRM practices survey contained scales developed by Snell and Dean (1992) to measure high commitment human resource practices: selective staffing measures the extensiveness of the firm's selection process; comprehensive training measures the extensiveness of the firm's training and development process; developmental appraisal measures whether performance appraisal is used for developing employees; externally equitable reward systems measured the extent to which the organization's pay levels were competitive with similar organizations; and internally equitable reward systems measured the extent to which the organization's pay structure was equitably construed.

Behavioral intent to comply privacy policy was represented by five reflective scale items. These scale items were originally developed by Fishbein and Ajzen (1975), and have since been used to predict a range of human behaviors (Sheppard *et al.*, 1988). Scales ranged from 1 to 5 but the anchors varied depending on the question. An additional eight questions were included for collecting demographic information such as gender, age, and workplace characteristics.

4. Results

We rely on multiple regression analyses for hypothesis testing. To test our regression models we used SPSS. Table 1 shows the result of our analysis. The model 1 inserts only all of control variables. The dependent variable is privacy policy compliance intent. It was found that organization tenure and training recency were significant ($\beta=0.1321$, $p<0.05$ and $\beta=0.2213$, $p<0.05$, respectively). The model 2 inserts all of independent variables. All of independent variables such as development-oriented are positively associated with privacy policy compliance intent as model 2 shows.

Table 1. The Effects of HRM Practices on Privacy Policy Compliance Intent

	Models	
	1	2
Job title	.61	.51
Organizational tenure	.24*	.21*
Length of career	.05	.03
Gender	.16	.11
Age	.25	.21
Training recency	.21*	.16*
Format of training	.31	.23
Total number of employees	.25	.21
Development-oriented appraisal		.32*
Externally equitable reward		.28*
Internally equitable reward		.30*
Selective staffing		.16*
Comprehensive training		.30*
Adjusted R^2	0.01	0.46
ΔR^2		0.45
ΔF		7.25

N=257, $|P|<0.05$ *, $|P|<0.01$ ** , Two-tailed tests

5. Discussions

The results of this study provide strong evidence for understanding the influence of a social exchange on employee perceptions of information privacy policy compliance intentions. The results show that an employee's compliance intentions are formed from the HRM practices within organizations. These results can also provide guidance for both managers and researchers involving employee policy compliance, in general, and information privacy policy compliance, specifically.

5.1. Managerial Implications

Managers who wish to improve individual information privacy compliance should consider a program to improve employee perceptions of social exchange about policy compliance. Such a program should focus on HRM practices which affect employee attitudes. Surprisingly, even though they can be a cost-effective means of improving outcomes, HRM practices are not often considered.

Employees committed to an organization are likely to play a role in his/her engagement in security behaviors. Therefore, Managers wishing to improve individual information privacy compliance need to enhance employees' commitment to organizations through HRM practices. Based on the results of this study, they should consider adopting the systems of developmental-oriented appraisal, externally or internally equitable reward, selective staffing and training for career development.

5.2. Research Implications

The uniqueness of this study is the application of social exchange theory to examine the influence of HRM practices on employee compliance outcomes. And it does provide numerous opportunities for future research in this area. For instance, while the majority of compliance research has focused on technical protection, very few studies have focused on the managerial aspects of a workplace and how HRM practices within these workspace impacts employee beliefs, attitudes, and perceptions related to compliance activities. As is evident from the results of this study, social exchange theory provides a useful lens for conceptualizing the interactions that take place between an employee and HRM practices. Also, social exchange theory can be applied within the policy compliance context to determine the long-term effects of an HRM practices on compliance outcomes, perhaps uncovering attenuating or intensifying effects over time.

5.3. Future Research Directions

This study provides HRM practices for establishing the antecedents of privacy compliance intent. Conducted among bank employees, its results can easily be generalized to other employees who must observe protocols to protect the privacy of other individual-level information. However, there are several limitations in our research and they offer opportunities for future research to continue this work. Though this study had over 200 respondents, they came from a handful of bank-related organizations and further research need to be conducted within a large variety of organizations of all types throughout the country. Further, if possible, the actual link between HRM practices and behavior (actual compliance) need to be established in this context. For example, laboratory experiments could be conducted to measure whether those employees who report higher levels of intent will actually safeguard information more closely. Finally, it is possible that organizational size is an important antecedent. For example, if small organizations have smaller budgets for information protection, but information-protective culture can be more important. Future research could be the comparative investigation of large and small enterprises regarding the relationship between organizational security budgets and organizational culture.

6. Conclusions

The results of this investigation provide guidance to all managers concerned with regulatory compliance involving individual employee behavior. To ensure that the staff actually complies with the privacy policy, managers must pursue technical and behavioral controls that have been proven to be effective in supporting the goals.

Our results show that HRM practices do influence employee's privacy compliance intent by manipulating the degree to which the employees perceive their social exchange relationship to carry out compliance activities. And they suggest that organizations can provide HRM practices that facilitate high levels of privacy compliance intent by developmental-oriented appraisal, externally or internally equitable reward, selective staffing and training for career development.

In summary, as concerns over privacy regulations continue to increase top managers must ensure that their employees are properly supported in the management of sensitive data. Maximizing the effectiveness of HRM practices is critical to the success of each employee and the entire organization toward compliance with privacy provisions. As such, management must consider any and all factors which may influence employee exchanging outcomes, including HRM practices. This study identified five HRM practices that have the potential to positively influence how employees react to their organizations and subsequently improve privacy policy compliance intent.

References

- [1] R. Agarwal and T. W. Ferratt, "Coping with labor scarcity in IT: Strategies and practices for effective recruitment and retention", Cincinnati, OH: Pinnaflex, (1999).
- [2] E. Albrechtsen, "A qualitative study of users' view on information security", *Computers & Security*, vol. 26, no. 4, (2007), pp. 276-289.
- [3] C. Anderson, "Creating the conscientious cybercitizen: an examination of home computer user attitudes and intentions towards security", Tenth INFORMS Conference on Information Systems and Technology (CIST) San Francisco, California, USA, (2005).
- [4] H. Angle, "Organizational commitment: Individual and organizational influences". *Sociology of Work and Occupations*, vol. 10, (1983), pp. 123-146.
- [5] J. B. Arthur, "Effects of human resource systems on manufacturing performance and turnover", *Academy of Management Journal*, vol. 37, (1994), pp. 670-687.
- [6] P. M. Blau, "Exchange and power in social life", New York: Wiley; (1964).
- [7] M. Chan, I. Woon and A. Kankanhalli, "Perceptions of information security at the workplace: linking information security climate to compliant behavior", *Journal of Information Privacy and Security*, vol. 1, no. 3, (2005), pp. 18-41.
- [8] K.-K. R. Choo, "The cyber threat landscape: challenges and future research directions", *Computers & Security*, vol. 30, no. 8, (2011), pp. 719-31.
- [9] J. D'arcy and A. Hovav, "The role of individual characteristics on the effectiveness of IS security countermeasures", Tenth Americas Conference on Information Systems New York; (2004).
- [10] G. Dhillon and G. Torkzadeh, "Value-focused assessment of information system security in organizations", *Information Systems Journal*, vol. 16, no. 3, (2006), pp. 293-314.
- [11] R. Eisenberger, R. Huntington, S. Hutchison and D. Sowa, "Perceived organizational support", *Journal of Applied Psychology*, vol. 71, (1986), pp. 500-507.
- [12] J. Finch, S. Furnell and P. Dowland, "Assessing IT security culture: system administrator and end-user perspectives", *Proceedings of ISOneWorld 2003 Conference and Convention Las Vegas, Nevada, USA, (2003)*.
- [13] M. Fishbein and I. Ajzen, "Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research", Addison-Wesley, Reading, MA, (1975).
- [14] S. M. Furnell, P. Bryant and A. D. Phippen, "Assessing the security perceptions of personal internet users", *Computers & Security*, vol. 26, no. 5, (2007), pp. 410-417.
- [15] B. Gomolski, "Management update: Tips to identify successful candidates for telecommuting", *InSide Gartner Group [newsletter]*, (2000).
- [16] S. R. Jaiswal, "Impact of organizational culture on commitment to work", *Lok Udyog*, vol. 16, (1982), pp. 3-14.
- [17] K. J. Knapp, T. E. Marshall, R. K. Rainer and F. N. Ford, "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness (ISC)2 Inc.", Palm Harbor, Florida and Auburn University, Auburn, Alabama, (2005).

- [18] G. H. Harel and S. S. Tzafrir, "The effect of human resource management practices on the perceptions of organizational and market performance of the firm", *Human Resource Management*, vol. 38, (1999), pp. 185-200.
- [19] G. C. Homans, "Social behavior", New York: Harcourt, Brace, and World, (1961).
- [20] C. Ichniowski, K. Shaw and G. Prennushi, "The effects of human resource management practices on productivity", *American Economic Review*, vol. 87, (1997), pp. 291-313.
- [21] A. L. Kalleberg and J. W. Moody, "Human resource management and organizational performance", *American Behavioral Scientist*, vol. 37, (1994), pp. 948-962.
- [22] F. Kerlinger, "Foundations of Behavioral Research", 2nd edn, Holt Reinhart & Winston, London, UK, (1973).
- [23] Laabs II. HR initiatives support Bell Helicopter's new plant operations. HRHQ.com [http://www.hrhq.com/members/archive/2490.html], (1997).
- [24] E. E. Lawler and G. D. Jenkins, "Strategic reward systems", D. M. Dunnette & M. L. Hough (Eds.), *Handbook of industrial organizational psychology*, Palo Alto, CA: Consulting Psychologists Press, vol. 3, (1992), pp. 1009-1055.
- [25] J. Leach, "Improving user security behavior", *Computers & Security*, vol. 22, no. 8, (2003), pp. 685-692.
- [26] S. M. Lee, S. G. Lee and S. Yoo, "An integrative model of computer abuse based on social control and general deterrence theories", *Information and Management*, vol. 41, no. 6, (2004), pp. 707-718.
- [27] H. Levinson, "Reciprocation: the relationship between man and organization", *Administrative Science Quarterly*, vol. 9, (1965), pp. 370-390.
- [28] K. D. Loch, H. H. Carr and M. E. Warkentin, "Threats to information systems: today's reality, yesterday's understanding", *MIS Quarterly*, vol. 16, no. 2, (1992), pp. 173.
- [29] J. P. Macduffie, "Human resource bundles and manufacturing performance: organizational logic and flexible production systems in the world auto industry", *Industrial and Labor Relations Review*, vol. 48, (1995), pp. 197-221.
- [30] M. G. Mcevoy, "Organizational change and outdoor management education", *Human Resource Management*, vol. 36, (1997), pp. 235-250.
- [31] Q. Ma and J. M. Pearson, ISO 17799: 'Best practices' in information security management? *Communications of the Association for Information Systems*, vol. 15, (2005), pp. 577-591.
- [32] W. H. Mobley, "Employee turnover: Causes, consequences, and control", Reading, MA: Addison Wesley, (1982).
- [33] C. J. Mottaz, "Determinants of organizational commitment", *Human Relations*, vol. 41, (1988), pp. 467-482.
- [34] R. T. Mowday, "Reflections on the study and relevance of organizational commitment", *Human Resource Management Review*, vol. 4, (1998), pp. 387-401.
- [35] R. T. Mowday, L. Porter and R. Steers, "Organizational linkages: The psychology of commitment, absenteeism, and turnover", New York: Academic Press, (1982).
- [36] J. Ogilvier, "The role of human resource management practices in predicting organizational commitment", *Group and Organizational Studies*, vol. 11, (1986), pp. 335-359.
- [37] C. Ostroff and D. E. Bowen, "Moving HR to a higher level: HR practices and organizational effectiveness", K. J. Klein & S. W. J. Kozlowski (Eds.), *Multilevel theory, research, and methods in organizations: foundations, extensions, and new directions* San Francisco: Jossey-Bass, (2000), pp. 211-266.
- [38] S. Pahnla, M. Siponen and A. Mahmood, "Employees' behavior towards IS security policy compliance", 40th Hawaii International Conference on System Sciences (HICSS 07) Hawaii, USA, (2007).
- [39] J. Pfeffer, "The human equation: Building profits by putting people first", Boston: Harvard Business School Press, (1998).
- [40] P. M. Podsakoff, "Organ D. Self-reports in organizational research: problems and prospects", *Journal of Management*, vol. 12, no. 4, (1986), pp. 531-544.
- [41] P. M. Podsakoff, S. B. Mackenzie, J. Y. Lee and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, vol. 88, no. 5, pp. 879-903.
- [42] C. Posey, R. J. Bennett and T. L. Roberts, "Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes", *Computers & Security*, vol. 30, no. 6-7, (2011), pp. 486-97.
- [43] G. V. Post and A. Kagan, "Evaluating information security tradeoffs: restricting access can interfere with user tasks", *Computers & Security*, vol. 26, no. 3, (2007), pp. 229-237.
- [44] L. Rennie, "Research note: detecting a response set to likert-style attitude items with the rating model", *Education Research and Perspectives*, vol. 9, no. 1, (1982), pp. 114-118.
- [45] M. A. Sasse, S. Brostoff and D. Weirich, "Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security", *BT Technology Journal*, vol. 9, no. 3, (2001), pp. 122-131.
- [46] R. P. Settoon, N. Bennett and R. C. Liden, "Social exchange in organizations: perceived organizational support, leader-member exchange, and employee reciprocity", *Journal of Applied Psychology*, vol. 81, (1996), pp. 219-227.

- [47] B. Sheppard, J. Hartwick and P. Warshaw, "The theory of reasoned action: a meta-analysis of past research with recommendations for modifications and future research", *Journal of Consumer Research*, vol. 15, no. 3, (1988), pp. 325-343.
- [48] K. Singh, "Effect of human resource management practices on firm performance in India", *Indian journal of Industrial Relations*, vol. 36, (2000), pp. 1-23.
- [49] S. Snell and J. Dean, "Integrated manufacturing and human resource management: a human capital perspective", *Academy of Management Journal*, vol. 35, (1992), pp. 467-504.
- [50] J. M. Stanton, K. R. Stam, I. Guzman and C. Caldera, "Examining the linkages between organizational commitment and information security", *IEEE Systems, Man, and Cybernetics Conference Washington DC, USA*, (2003).
- [51] J. M. Stanton, K. R. Stam, P. Mastrangelo and J. Jolton, "Analysis of end user security behaviors", *Computers & Security*, vol. 24, no. 2, (2005), pp. 124-133.
- [52] R. Steers and D. Spencer, "The role of achievement motivation in job design", *Journal of Applied Psychology*, vol. 62, (1977), pp. 472-479.
- [53] D. W. Straub, "Effective is security: an empirical study", *Information Systems Research*, vol. 1, no. 3, (1990), pp. 255-276.
- [54] D. W. Straub and R. W. Collins, "Key information issues facing managers: software piracy, proprietary databases, and individual rights to privacy", *MIS Quarterly*, vol. 14, no. 2, (1990), pp. 143-156.
- [55] D. Ulrich, "Measuring human resources: An overview of practice and a prescription for results", *Human Resource Management*, vol. 36, (1997), pp. 303-320.
- [56] C. Vroom and R. von Solms, "Towards information security behavioral compliance", *Computers & Security*, vol. 23, no. 3, (2004), pp. 191-198.
- [57] R. E. Walton, "From control to commitment in the workplace", *Harvard Business Review*, vol. 63, no. 2, (1985), pp. 77-84.
- [58] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat", *European Journal of Information Systems*, vol. 18, no. 2, (2009), pp. 01-105.
- [59] M. L. Weitzman and D. L. Kruse, "Profit sharing and productivity", A. S. Blinder (Ed.), *Paying for productivity Washington, DC: Brookings Institution*, (1990), pp. 95-142.
- [60] S. Wood, L. de Menezes, "High commitment management in the U.K.: evidence from the Workplace Industrial Relations Survey and Employers' Manpower and Skills Practices Survey", *Human Relations*, vol. 51, (1998), pp. 485-515.
- [61] M. Youndt, S. Snell, J. Dean and D. Lepak, "Human resource management, manufacturing strategy, and firm performance", *Academy of Management Journal*, vol. 39, (1986), pp.836-866.
- [62] H. Zafa and J. G. Clark, "Current state of information security research in IS", *Communications of the Association for Information Systems*, vol. 24, no. 34, (2009), pp. 557-596.
- [63] X. Zhang, "What do consumers really know about spyware", *Communications of the ACM*, vol. 48, no. 8, (2005), pp. 44-48.

