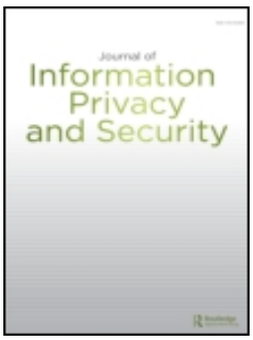

Journal of Information Privacy and Security

ISSN: 1553-6548 (Print) 2333-696X (Online) Journal homepage: http://www.tandfonline.com/loi/uips20

Job Quitters, Information Security Awareness, and Knowledge Management Strategies

Hongbo Lyu & Zuopeng (Justin) Zhang

To cite this article: Hongbo Lyu & Zuopeng (Justin) Zhang (2015) Job Quitters, Information Security Awareness, and Knowledge Management Strategies, Journal of Information Privacy and Security, 11:4, 189-210, DOI: 10.1080/15536548.2015.1105594

To link to this article: http://dx.doi.org/10.1080/15536548.2015.1105594

Published online: 22 Dec 2015.

Submit your article to this journal

Article views: 15

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=uips20

Download by: [University of New England] **Date:** 15 March 2016, At: 02:50

Journal of Information Privacy and Security, 11: 189–210, 2015
Published with license by Taylor & Francis
ISSN: 1553-6548 print / 2333-696X online
DOI: 10.1080/15536548.2015.1105594

Routledge
Taylor & Francis Group

ARTICLES

Job Quitters, Information Security Awareness, and Knowledge Management Strategies

Hongbo Lyu
Modern Logistics School, Zhejiang Wanli University

Zuopeng (Justin) Zhang
School of Business and Economics, State University of New York

Downloaded by [University of New England] at 02:50 15 March 2016

Information security culture plays a crucial role in improving employees' security awareness within a firm. Knowledge management initiatives can help transform culturally unfit workers into those who will possess the necessary level of security awareness and are aligned with a firm's information security culture. This research analytically models and studies the best knowledge management performance quotient (KMPQ) in a firm to convert workers who are unfit into those who fit with its security culture in order to improve the firm's organizational level of security awareness (OLSA) and maximize its total payoff. When the potential security threat comes from all the workers who depart the firm, either voluntarily or involuntarily, findings in this study suggest that the firm should implement full knowledge management initiatives to achieve a KMPQ as high as possible if the loss from the security threat is less than a specific threshold level. This study further differentiates three sources of a security threat (voluntary unfit quitters, voluntary fit quitters, and involuntary quitters), and assesses the firm's best KMPQ accordingly. In addition, this article illustrates the implementation process of the firm's knowledge management strategies based on the study's decision framework. This research provides valuable guidance for practitioners to effectively implement knowledge management strategies to build a successful information security culture within organizations.

INTRODUCTION

In an information age, information can be easily accessible and shared over communication networks. The convenience of collecting and transferring information increases the vulnerability of

© Hongbo Lyu and Zuopeng (Justin) Zhang
Correspondence should be addressed to Zuopeng (Justin) Zhang, 206 Au Sable, Plattsburgh, NY 12901. E-mail: zzhan001@plattsburgh.edu

www.m

private and sensitive information that needs to be protected and kept confidential in organizations. It is not difficult for an organization to implement state-of-the-art security technologies and corresponding strategies to protect its corporate networks, data, and information assets as organizational security threats are commonly believed to come from the outside (Parks & Wigand, 2014). However, organizational users may make unintentional mistakes disrupting regular security services or be tricked by social engineers to divulge their confidential credentials.

Many studies (e.g., D'Arcy, Hovav, & Galletta, 2009) find that internal threats are the major sources of organizational data breaches because people are the central elements of security systems as they are the ones to capture, share, and utilize the data and information assets. For example, the report by Forrester, titled as "Understand the State of Data Security and Privacy", indicates insiders as the top source of security breaches with 36% resulting from workers' data misuse or carelessness. In addition, the report shows that only 42% of small- or medium-size business workers in North America or Europe have received training about information security awareness and only 57% are aware of the security policies in their companies (Hatchimonji, 2013).

In a similar survey from ecological momentary assessment research, 56% of workers indicate that they have not had any information security awareness training from their organizations, 58% use their personal storage device to save organizational sensitive information, 59% store their work related documents on clouds, 35% have clicked an link in emails from unknown senders, and 33% use the same password for home and office computers (Wilson, 2014). Therefore, it is important for organizations to establish an effective information security awareness program to education users about their responsibilities as the most crucial parts of security systems within organizations.

Many organizations focus their information security programs on their current employees, but fail to recognize the potential damages caused by a special group of insiders, the organization's former employees or job quitters, who may pose significant security threats. According to a survey by Courion, 93% of organizations do not think they need to worry about the security threats from their former workers and 53% are not aware that these workers may still have access to their information systems. In a related survey from Ipswitch File Transfer, 25% of people state that they have used their personal emails to store organizational files so as to use them in their next jobs (Dolan, 2010).

Many recently reported incidents of data breach were committed by former employees of organizations. For example, a man fired by a Texas car dealership broke into its customer base by using his former colleague's password and disabled more than 100 customers' car functions (Brazas, 2014). A former employee of the Park Hill School District in Kansas City, Missouri, downloaded all the files, including more than 10,000 individuals' private information, from his work computer to a personal hard drive and then connected it to his home network, resulting in all the files being temporarily accessible over the Internet (Roman, 2014). Another incident of a former employee's data breach took place at the University of Massachusetts Memorial Medical Center in Worcester. The hospital reported that one of its former staffs accessed protected health information for 2,400 patients, including their social security numbers, dates of birth, and credit card numbers (Cocchi, 2014).

Despite the increasing number of security breach incidents committed by former insiders, successful business practice is still lacking to prevent the happening of such breaches. Some recent studies (e.g., Lupiana, 2008) suggest that knowledge management can help build an

Downloaded by [University of New England] at 02:50 15 March 2016

المنارة للاستشارات
www.m

effective framework to cultivate an information security culture in order to train organizational employees and improve security awareness. Prior research (Maryam, Kayworth, & Leidner, 2005) shows that knowledge management and organizational culture are inseparable in terms of their mutual interactions within organizations. In particular, knowledge management practices improve organizational cultural fit, and organizational culture increases the perceived explicitness of knowledge, thus facilitating the implementation of knowledge management initiatives (Jasimuddin & Zhang, 2013).

However, prior studies have never systematically studied the role of knowledge management in nurturing information security culture through its facilitation of knowledge workers' awareness of security policies and procedures in organizations. The current study addresses this gap by formally considering the organizational security threats in a firm from its job quitters, analytically modeling its organizational level of security awareness, and investigating the best performance of knowledge management initiatives to promote information security culture and maximize its total payoff.

Specifically, this study addresses the following three major research questions:

- How does a firm's organizational information security awareness evolve over time?
- What is the firm's best knowledge management strategy to improve its organizational information security awareness, maximizing its total payoff?
- How should the firm implement its best knowledge management strategies?

This discussion proceeds as follows. The next section reviews prior literature. The third section presents an analytical model capturing the major features of knowledge management strategies related to information security culture and awareness. The fourth section details the analysis of the model by investigating the best organizational decision on knowledge management strategies. The last section concludes the entire article.

LITERATURE

This section reviews prior related research. First summarized are the major findings from two research streams: (1) information security awareness and knowledge management, and (2) organizational culture and knowledge management, and then this article differentiates this research and highlight this contributions.

Research shows that workers who comply with the security rules and regulations in organizations are crucial to the success of information security (Bulgurcu, Cavusoglu, and Benbasat, 2010). Therefore, the two seemingly irrelevant fields, information security management and knowledge management, share a lot of interesting commonalities, which makes it possible for these two fields to borrow solutions to solve problems from each other (Glaser & Pallas, 2007). For example, Kesh and Ratnasingam (2007) claim that the major advantage of knowledge management enables organizations to identify appropriate mechanisms to address the needs of knowledge capture, transfer, and applications, which bears significant implications for security management in organizations. D'Arcy et al. (2009) suggest that security education, training, and awareness (SETA) program is one of the effective practices to deter information security misuse within organizations. He, Yuan, and Yang (2013) demonstrate that case-based learning is an effective method for security management education. Mejias and Balthazard (2014) indicate that

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

technical knowledge in an organization positively correlates with its information security awareness. Kesar (2008) shows that managers' knowledge about a company's structure, functions, and purposes greatly impact the ways and performance of information security management within the company, as managers have the abilities to influence other workers to implicitly remind them of the information security policies and processes, which exemplified the importance of developing and utilizing tacit knowledge. Conklin and McLeod. (2009) introduce the essential body of knowledge framework (from national strategy to secure cyberspace) in terms of its contents and form and demonstrate how it can be used to establish security architecture in an organization to satisfy its security needs. Lupiana (2008) finds that knowledge management systems can provide a valuable framework to encourage users to participate in security education so as to improve employees' awareness of security policies and ethics in organizations. Building upon the universal constructive instructional theory and the elaboration likelihood model, Puhakainen and Siponen (2010) propose a training program to improve employees' compliance with organizational security policies and validate its efficacy. The researchers Mookerjee et al. (2011) analyze the impact of security knowledge dissemination among hackers to the management of a detection system in a firm and find that under certain conditions hackers do not benefit from the dissemination of such knowledge.

In a reverse direction, information security management also has great implications for knowledge management. For example, Jennex and Zyngier (2007) argue that various models of security and risk management (e.g., the National Security Telecommunications and Information Systems Security Committee) can be integrated into knowledge management success models to formulate mechanisms for KM support, governance, and strategies. Ting, Woon, and Kankanhalli (2005) study the relationship between security issues and knowledge management systems and empirically demonstrate that security training greatly affects the perceived usefulness of knowledge management systems through several mediating factors including security self-efficacy. In contrast, the security level of knowledge management systems determines its perceived ease of use. While prior research in this stream describes the relationship between knowledge management and information security awareness, this current study investigates the implementation of knowledge management strategies in improving organizational level of security awareness.

Many studies have explored the mutual interactions and effects between organizational culture and knowledge management. For example, Park, Ribiere, and Schulte (2004) summarize the crucial organizational factors enabling knowledge sharing and facilitating the implementation of knowledge management technologies. Lemken, Kahler, and Rittenbruch (2000) find that an organizational culture promoting knowledge sharing allows organizations to adapt to changing environments. Donate and Guadamillas (2010) claim that organizational culture serves as different types of moderators when firms implement different knowledge management initiatives in storing and transferring organizational knowledge. Investigating four types of organizational cultures (i.e., clan, adhocracy, market, and hierarchy), Fong and Kwok (2009) study their effects on the knowledge flow and the success of knowledge management systems in different organizations. Based on a case study, Maryam et al. (2005) explore the impact of organizational culture on knowledge management practices with a focus on the use of knowledge management technologies. Leidner, Alavi, and Kayworth (2006) analyze how organizational cultures influence two knowledge management approaches (organizing communities and knowledge management processes) and show that knowledge initiatives can result in either an information repository or electronic communities. Jasimuddin and Zhang (2013) identify two strategies based

Downloaded by [University of New England] at 02:50 15 March 2016

المنارة للاستشارات
www.m

on knowledge tacitness and recommend a symbiosis strategy for companies to develop a unique organizational culture which prevents imitations from competitors. While prior studies have focused on the impact of organizational culture on knowledge management, the authors of this current study want to incorporate the element of information security awareness and investigate how its mutual interactions with knowledge management strategies and security cultures.

In summary, prior research provides a solid foundation for us to understand the fundamental relationship among knowledge management, information security awareness, and organizational cultures. This study synthesizes the elements from prior studies and creates an analytical model to explore the optimal knowledge management initiatives to cultivate an organization's information security culture through improving its employees' awareness of security policies and procedures.

Downloaded by [University of New England] at 02:50 15 March 2016

MODEL

This section presents an analytical model of improving workers' security awareness in organizations through knowledge management initiatives. First delineated is the setting of the model, then demonstrate the firm's decision problem as a base model, and finally describe the framework that incorporates the variations of the base model for analysis and discussion. All the notations for this model can be found in Table 1.

A firm hires knowledge workers (measure at 1) from a labor market to perform a series of tasks for n periods of time. On the labor market, S_0 percent of the workers have the knowledge about the firm's security policies, regulations, and code of ethics, satisfying the minimal individual security compliance required by the firm. The percentage of knowledge workers who understand and comply with the firm's information security culture including its security policies, regulations, and code of ethics is denoted as a firm's organizational level of security awareness (OLSA). Note that the firm's OLSA at the beginning is S_0. In addition, this study considers the workers who are fit with the firm's information security culture as those who possess the necessary level of information security awareness.

TABLE 1
Summary of Notation

Δ	difference of high and low outputs
S_0	initial OLSA (organizational level of security awareness)
S_i	OLSA in time period i
r	probability of a worker being identified as unfit and removed in each period
q	probability of a worker staying in the firm in each period
p_i	KMPQ (knowledge management performance quotient), the probability of a culturally unit worker being transformed into a fit one in time period i
t	index of time periods
w	fixed wage payment for workers in each period
O_L	output from culturally unfit workers
O_H	output from culturally fit workers

www.m

In each period, an employed worker will generate a high production output O_H if she has the mandatory security knowledge (i.e., the information security awareness), and $O_L = O_H - \Delta$ otherwise. For example, a worker who does not comply with the firm's security policies and regulations may be less productive by losing her valuable production times in order to fight with computer virus infections and other consequences of security non-compliances. A worker receives a wage payment w in each period, with the assumption that $w > O_L$.

At the end of each period, a worker will stay and continue to work for the firm in the following period with the probability q. In addition, the firm evaluates workers with respect to their security compliances by the end of each period; those with insufficient level of information security awareness will be identified with the probability r and removed by the firm. The diminished workforce will be replenished from the same labor market.

The workers who leave the firm, either voluntarily or unwillingly, will pose a potential threat to the firm's overall security system. In particular, it is considered that former employees may disclose the details of the firm's system vulnerabilities and other important information to the firm's competitors, resulting in a potential financial loss λ to the firm with the probability $\alpha(L_i)$, where L_i is the total percentage of workers who depart the firm in the i^{th} time period.

$$L_i = (1 - S_{i-1})(1 - p_i)(1 - q) + (1 - S_{i-1})(1 - p_i) \cdot q \cdot r + [S_{i-1} + (1 - S_{i-1})p_i] \cdot (1 - q)$$

The firm applies appropriate knowledge management strategies to facilitate knowledge sharing and learning among hired workers in each period so that those workers who do not have sufficient security knowledge may reach the required level of security awareness after learning either from the knowledge base or from other workers with a sufficient level of security awareness. Based on the knowledge management initiatives implemented by the firm in the i^{th} time period, p_i proportion of initially unfit workers will become fit with the firm's information security culture. Akin to the concept in Jasimuddin and Zhang (2013), the proportion p_i is defined as the *knowledge management performance quotient* (*KMPQ*) in the i^{th} time period, which measures the percentage of cultural unfit workers being transformed into fit ones, depending on the effort exerted by the firm in promoting the knowledge transfer within the firm.

In summary, the firm's decision problem [P] is to determine the best KMPQ p_i in each period to maximize its total payoff in n time periods, which is:

$$\max_{p_i} \quad \pi = \sum_{i=1}^{n} \beta^{i-1}\{(O_L - w) + S_i \cdot \Delta - \lambda \cdot \alpha(L_i)\}. \tag{EQ1}$$

This base model represented as the firm's problem [P] will be analyzed in the following section. In addition, this study investigated the variations of the problem [P] along the following two dimensions: (1) the source of the potential security threat, and (2) the consistency of the KMPQ in each period. The first dimension identifies four different categories of security threat sources:

- All quitters: all the workers who quitting the firm;
- Voluntary unfit quitters: workers who are not fit with the firm's security culture and voluntarily quit the firm;
- Voluntary fit quitters: workers who are congruent with the firm's security culture and voluntarily quit the firm; and

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

TABLE 2
The Two-Dimensional Framework for Analysis

		Consistency of KMPQ	
	Heterogeneous	*Homogeneous*	
Source of Security Threats	All quitters	§ 4.2.1	§ 4.3
	Voluntary unfit quitters	§ 4.2.2	
	Voluntary fit quitters	§ 4.2.4	
	Involuntary quitters	§ 4.2.3	

- Involuntary quitters: workers who are unfit with the firm's security culture and want to stay but are identified and removed by the firm.

The second dimension differentiates the KMPQ in each period to be either homogeneous (consistent p_i) or heterogeneous (inconsistent p_i). Table 2 summarizes the variations of the base model and the sections in which they will be investigated.

ANALYSIS AND DISCUSSION

This section details the analysis and discussion of the firm's decision problem [P]. This research studies the organizational level of security awareness (OLSA) in each period regarding its change with different factors, explores the firm's optimal decision for various scenarios, discusses the implementation of knowledge management strategies, and finally highlights the contributions and limitations of the study in response to the three primary research questions

Olsa

The organizational level of security awareness (OLSA) S_i in each period can be derived as:

$$S_i = [S_{i-1} + (1 - S_{i-1})p_i] \cdot q + \{(1 - S_{i-1})(1 - p_i)(1 - q) + (1 - S_{i-1})(1 - p_i) \cdot q \cdot r + [S_{i-1} + (1 - S_{i-1})p_i] \cdot (1 - q)\} \cdot S_0, \quad \text{(EQ2)}$$

where:

- The first term represents all the workers who are fit with the firm's information security culture (including those who become fit through the firm's knowledge management initiatives) and want to stay in the firm;
- The second term corresponds to those who are not fit with the firm's information security culture and want to quit;
- The third term stands for those who are not culturally fit and want to continue working for the firm, but are removed because they are identified as being unfit with the firm's information security culture; and

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

- The last term describes those who are fit but want to leave the firm.

Proposition 1. *The organizational level of security awareness (OLSA) S_i increases with the rate q of workers remaining in the firm, the probability r of a worker being identified as a cultural unfit worker, and the KMPQ p_i in the current period.*
Proof (Appendix A). ■

Proposition 1 demonstrates how the organizational level of security awareness changes with some of the crucial organizational factors. Specifically, when more workers are willing to remain in the firm, the information security culture of the firm tends to stabilize so more workers will have the necessary security awareness. In addition, the organizational level of security awareness gets improved when more culturally unfit workers are identified and removed by the firm or when the firm implements its knowledge management initiatives to convert more cultural unfit workers into those being congruent with the firm's information security culture.

Based on the firm's OLSA in each period, the effect of KMPQ on OLSA in each period is studied next. When $p_i = 1$, the firm achieves a highest KMPQ; when $p_i = 0$, the KMPQ is the lowest. Since OLSA increases in KMPQ in each period, it is shown in the following proposition the maximal improvement of OLSA between these two cases of KMPQ.

Proposition 2. *The maximal improvement of the organizational level of security awareness (OLSA) through knowledge management initiatives in a time period i is $q(1 - rS_0)(1 - S_{i-1})$.*
Proof (Appendix B). ■

Proposition 2 illustrates the impact of knowledge management initiatives to the firm's organizational level of security awareness (OLSA), which implies that the firm's ability r in identifying workers who are unfit with its security culture and the initial organizational level of security awareness S_0 are complements of the knowledge management initiatives in improving the firm's OLSA. In addition, Proposition 2 suggests that it is important to retain workers in the firm so as to reap the maximal benefits of knowledge management initiatives in building up the firm's OLSA.

Having studied the OLSA in each period, next considered is the scenario in which KMPQ is consistent in each period, i.e., $p_i = p$, and the OLSA is explored for this case, which is summarized in the following proposition.

Proposition 3. *When the KMPQ in each period are the same (i.e., $p_i = p$), the firm's organizational level of security awareness in a long run is*

$$S_\infty = \frac{[1 - q + qr(1 - p)]S_0 + qp}{1 - q(1 - p)(1 - rS_0)},$$

which increases with the rate q of workers remaining in the firm, the probability r of a worker being identified as a cultural misfit, the KMPQ p in the current period, and the initial OLSA S_0.
Proof (Appendix C). ■

Proposition 3 displays the closed-form solution for the OLSA when the time goes to infinity under the scenario that KMPQ is homogeneous in each period. The OLSA in this case changes with the identified factors (r, q, p) in the same way as the OLSA in Proposition 1. Next investigated is the optimal KMPQ in the following subsection; both of the cases when KMPQ in each period is heterogeneous or homogeneous will be discussed.

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

Optimal Heterogeneous KMPQ

The firm's optimal KMPQ in each period is derived in this subsection. Beginning with the base model for the firm's decision problem [*P*], this study then investigates three variations of the base model when the potential security threat comes from culturally fit workers who voluntarily quit the firm, culturally unfit workers who voluntarily choose to leave the firm, or culturally unfit workers who are identified and removed by the firm.

Base Model

To simplify the analysis without losing meaningful insights, it is assumed that the probability function $\alpha(L_i)$ of the firm incurring a loss due to the security threats as $\alpha(L_i) = L_i$. The following proposition demonstrates the best KMPQ that the firm should choose in each period under certain conditions.

Proposition 4. *When the potential security threat* λ *comes from all the workers who leave the firm, the firm should implement its knowledge management initiatives to achieve a KMPQ as high as possible in each period if:*

$$\lambda > \lambda' = S_0\Delta + \frac{O_L - w + q\Delta}{1-q}, \text{ or} \tag{EQ3}$$

$$q > \frac{\lambda - S_0\Delta - (O_L - w)}{\lambda - S_0\Delta + \Delta}. \tag{EQ4}$$

Proof (Appendix D). ■

Proposition 4 presents the best KMPQ for the firm's decision problem in the base model in which all the workers who depart the firm in each period will collectively pose a security threat, resulting in a potential loss λ to the firm. The condition in Inequality (3) shows that the firm will fully implement its knowledge management initiatives only if the loss λ is less than a threshold level $S_0\Delta + (O_L - w + q\Delta)/(1-q)$; otherwise, the knowledge management initiatives should not be taken at all because the firm will not benefit from them. The threshold level increases in several parameters including S_0, Δ, and q, which implies that the firm should always take advantage of its knowledge management practice when its initial OLSA is high, when more workers are willing to stay in the firm, or when the difference between the low and high output is larger.

Voluntary Unfit Quitter

Next explored is the firm's optimal KMPQ when the potential security threat comes from workers who voluntarily quit the firm and are misaligned with the firm's information security culture, which is shown in the following proposition.

Proposition 5. *When the potential security threat* θ *comes from the cultural unfit workers who voluntarily quit the firm, the firm should implement its knowledge management initiatives to achieve a KMPQ as high as possible in each period.*
Proof (Appendix E). ■

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

Proposition 5 shows how the best KMPQ the firm should achieve when the security threat is derived from all culturally unfit workers who voluntarily depart the firm. The result of Proposition 5 is intuitive because if all the culturally unfit workers are transformed into culturally fit ones in each period, then the firm will not worry about the potential loss from the security threats posed by culturally unfit workers who voluntarily depart the firm as there will be no voluntary unfit quitters in each period.

Involuntary Quitter

Further studied is the scenario when only those cultural unfit workers who are identified and removed by the firm may cause the security concern. The following proposition presents the optimal KMPQ in each period for such case.

Proposition 6. *When the potential security threat δ comes from workers who are removed by the firm as they are identified as misaligned with the firm's security awareness requirements, the firm should implement its knowledge management initiatives to achieve a KMPQ as high as possible in each period.*
Proof (Appendix F). ■

Proposition 6 bears the same insight as that in the previous proposition. It makes no difference to the firm whether the workers voluntarily or involuntarily depart the firm; as long as they are incongruent with the firm's information security culture, the firm should take its knowledge management initiatives to achieve a highest KMPQ in each period so as to guarantee that all cultural unfit workers are transformed into fit ones and will have the necessary information security awareness. Therefore, the potential security threat from cultural unfit workers will be completely eliminated.

Voluntary Fit Quitter

Finally investigated is the best KMPQ in each period for the case when the potential security threat is posed by workers who are fit with the security culture but wants to leave the firm, which is summarized by the following proposition.

Proposition 7. *When the potential security threat φ comes from the workers who quit the firm and are well aligned with its security awareness requirements, the firm should implement its knowledge management initiatives to achieve a KMPQ as high as possible in each period if*

$$\varphi < \varphi' = \frac{1 - rS_0}{1 - q} \cdot q\Delta. \tag{5}$$

Proof (Appendix G) ■

Proposition 7 demonstrates a similarly result of the firm's best KMPQ when the threat source is from voluntary fit job quitters as that in Proposition 4 when the source of the threat comes from all job quitters. As it can be observed that $\varphi' < \lambda'$, the range illustrated in Inequality (5) is essentially a subset of that in Inequality (3). As discussed in Proposition 5 and 6, the firm does not need to worry about the degree of loss for the security threats coming from cultural unfit workers.

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

Therefore, even if the source of the threats is from all job quitters, it is the group of culturally fit job quitters who actually requires the firm to evaluate the loss of the threats against a threshold.

Optimal Homogeneous KMPQ

A special case is studied of the firm's decision problem when the KMPQ is the same for all the time periods, i.e., $p_i = p$. The next proposition summarizes the result for this case.

Proposition 8. *For the homogeneous case, when the number of time periods goes into infinity, the firm should implement knowledge management initiatives to achieve a KMPQ as high as possible in each period, (1) if the security threat is from all job quitters and the degree of loss* λ *is*

$$\lambda > \lambda' = S_0\Delta + \frac{O_L - w + q\Delta}{1-q},$$

(2) if the source of the security threat is from voluntary unfit quitters, (3) if the threat is from involuntary quitters, or (4) if the threat is from voluntary fit quitters and the degree of loss φ *is*

$$\varphi < \varphi' = \frac{1 - rS_0}{1-q} \cdot q\Delta.$$

Proof show in Appendix (Appendix H).■

Proposition (8) shows that the best KMPQ for the homogeneous setting is the same as that for the heterogeneous setting, so the firm does not have to care about the consistency of its KMPQ in each period when determining the best knowledge management strategies for implementation.

Implementation of Knowledge Management Strategies

Having investigated the optimal KMPQ under different scenarios, next discussed is how the firm should implement its knowledge management strategies based on different threshold levels identified in previous subsections.

Table 3 presents a decision table that summarizes the knowledge management strategies under different conditions in which the following notations are used to represent four major sources of threats:

- A: All quitters,
- F: Voluntary fit quitters,
- U: Voluntary unfit quitters.
- I: Involuntary quitters,

and the hyphen "–" denotes the case when the firm is indifferent to the four sources of security threats. Five decision rules are summarized for the firm to take two types of knowledge management strategies: either full (i.e., KMRP $p_i = 1$) or no (i.e., KMRP $p_i = 0$) KM initiatives. Decision rules 1, 3, and 5 capture the conditions under which full KM initiatives should be taken: rule (1) when the loss of the potential security threat is below φ'; rule (3) when the loss of the potential security threat is between φ' and λ' and the source of the threat comes from voluntary unfit quitters (U), involuntary quitters (I), or all the quitters (A); and rule (5) when the loss of

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

TABLE 3
Decision Table for Knowledge Management Strategies

	Decision Rules				
Conditions	*1*	*2*	*3*	*4*	*5*
Sources of threats	—	F	A, U, or I	A or F	U or I
Degree of losses	$(-\infty, \varphi']$	$(\varphi', \lambda']$	$(\varphi', \lambda']$	$(\lambda', +\infty]$	$(\lambda', +\infty]$
Actions					
Full KM initiatives	X		X		X
No KM		X		X	

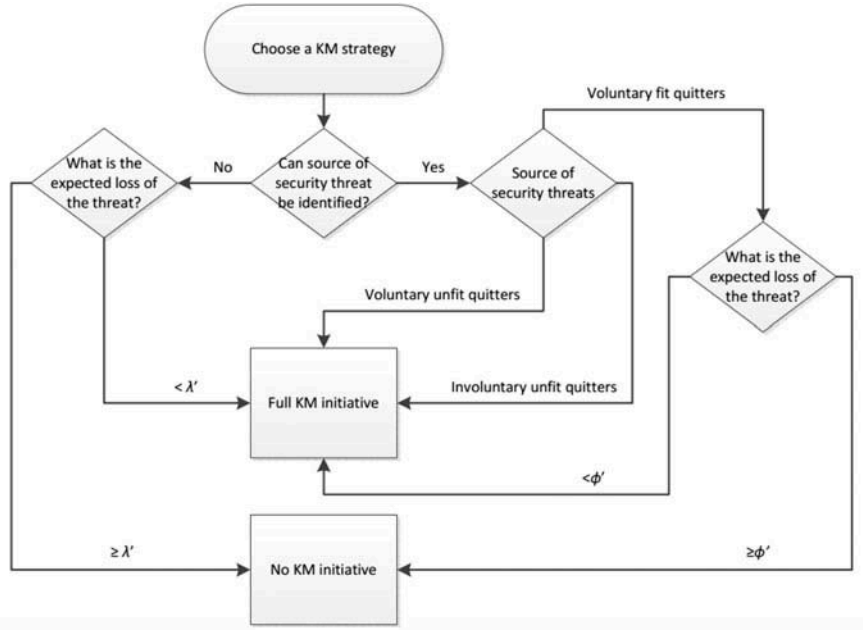

FIGURE 1 Process of implementing knowledge management initiatives.

the potential security thread is greater than λ' and the source of the threat comes from voluntary unfit (U) or involuntary quitter (I). Note that in decision rule (1) the firm does not have to care about the source of the potential security threat. Decision rules 2 and 4 represent the cases when no KM initiative should be implemented: rule (2) when the loss of the potential security threat is between φ' and λ' and the source of the threat comes from voluntary fit quitters (F); and rule (4) when the loss of the potential security thread is greater than λ' and the source of the threat comes from voluntary fit (F) or all the quitter (A).

The decision process is further presented for implementing the knowledge management strategies in Figure 1. The firm first evaluates the potential security threat to determine whether its source can be identified, from one of the following three sources: voluntary fit quitters, voluntary

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

unfit quitters, or involuntary quitters. If the firm cannot decide which group of quitters poses the potential security threat, the threat will be considered as collectively coming from all the quitters; hence, the next step is to assess the degree of loss from the security threat. The firm will implement full KM initiatives if the loss is less than λ'; otherwise, no KM initiative will be taken. In contrast, if the firm believes that the source of the threat is identifiable, either from voluntary unfit or involuntary quitters, the firm will always enact the full KM initiatives as it does not have to care about the degree of loss for the security threat. If the source of the threat is from voluntary fit quitters, the degree of loss for the threat needs to be assessed; full or no KM initiatives should be taken depending on whether the loss is less than or greater than φ'.

Contributions and Limitations

Finally, the contributions and limitations of this research are highlighted in this subsection. In response to the research questions raised in the first section, this study makes are following significant contributions to the current literature.

First, the evolving organizational level of security awareness over time is explored. The organizational level of security awareness is considered as the percentage of knowledge workers who possess necessary information security awareness, congruent with the current information security culture within organizations. The study found that the organizational level of security awareness (OLSA) increases with the probability of workers remaining in the firm, the rate of a worker being identified as a cultural unfit one, and the KMPQ in each period. In addition, the study derived the OLSA in the homogenous setting (i.e., when the KMPQ is the same in each period) and identified the same changing patterns of the OLSA with the identified factors.

Second, the firm's best knowledge management strategies were analyzed to improve its organizational information security awareness, maximizing its total payoff. The analysis differentiated along the following two dimensions: (1) the source of the potential security threat, and (2) the consistency of the KMPQ in each period. The first dimension identifies four different categories of security threat sources: all quitters, voluntary unfit quitters, voluntary fit quitters, and involuntary quitters; the second dimension differentiates the KMPQ in each period to be either homogeneous or heterogeneous. It was found that the firm should implement knowledge management initiatives to achieve a KMPQ as high as possible in each period when the source of security threats is from either voluntary unfit or involuntary quitters. The same knowledge management strategies should be implemented if the source of security threats is from either all job quitters or just voluntary fit quitters, but only when the degree of loss is within certain thresholds. In addition, it makes no difference in terms of the best knowledge management strategies between the homogeneous and heterogeneous KMPQ in each period.

Finally, the implementation process of the best knowledge management strategies identified was explored through the analytical framework. According to whether the security threat source can be identified, the firm determines its knowledge management strategies. If the firm cannot decide which group of quitters poses the potential security threat, the next step is to estimate the loss of security threats and then formulate its strategy accordingly. In contrast, if the source of the threat can be identified from either voluntary unfit or involuntary quitters, the firm will always implement the full KM initiatives; if the threat is expected to come from voluntary fit quitters, the loss of the threat also needs to be assessed so as to take appropriate KM initiatives.

Downloaded by [University of New England] at 02:50 15 March 2016

المنارة للاستشارات
www.m

However, these results and their derived insights are based on some crucial assumptions. Future research may relax some of these assumptions to mitigate the limitations of the paper and search for proper knowledge management strategies in more details. For example, the probability function of the potential security threats is considered as a linear function of the percentage of workers who leave the firm, which can be relaxed to investigate how sensitive the analytical results are in terms of the functional forms of the probability function.

CONCLUSION

Information security awareness is of great importance in organizations as many security breaches are committed by insiders. As a special group of insiders, former employees or job quitters of an organization pose significant security threats. However, there lacks specific research on appropriate knowledge management strategies that can promote employees' information security awareness so as to prevent such types of threats within organizations. This study addresses the research gap by formally considering the organizational security threats in a firm from its job quitters, analytically modeling its organizational level of security awareness, and investigating the best performance of knowledge management initiatives to nurture information security culture and maximize its total payoff. The analytical results provide valuable insights for practitioners to effectively manage knowledge assets to improve organizational security awareness and for researchers to build connections between knowledge management and information security.

FUNDING

This research is supported by Key Research Institute of Philosophy and Social Science of Zhejiang Province –Modern Port Service Industry and Creative Culture Research Center (No.13JDLG03YB) and the Technology Innovation team project of Ningbo (No.2012B82003).

REFERENCES

Brazas, S. M. (2014). Disgruntled employees can cause chaos, *Employer-Employee Relations at Lawyers.com*. Retrieved from http://labor-employment-law.lawyers.com/human-resources-law/disgruntled-employees-can-cause-chaos.html

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

Cocchi, R. (2014). Data breach: Former hospital employee accessed 2,400 patient records. *Healthcare Business & Technology*. Retrieved from http://www.healthcarebusinesstech.com/data-breach-hospital/

Conklin, W. A., & McLeod., A. (2009). Introducing the information technology security essential body of knowledge framework. *Journal of Information Privacy and Security*, *5*(2), 27–41. doi:10.1080/15536548.2009.10855862

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. doi:10.1287/isre.1070.0160

Dolan, P. L. (2010). Data breached? Culprit could be a former employee, *American Medical News*, Retrieved from http://www.amednews.com/article/20100419/business/304199962/5/

Donate, M. J., & Guadamillas, F. (2010). The effect of organizational culture on knowledge management practices and innovation. *Knowledge and Process Management*, *17*(2), 82–94. doi:10.1002/(ISSN)1099-1441

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

Fong, P. S. W., & Kwok, C. W. C. (2009). Organizational culture and knowledge management success at project and organizational levels in contracting firms. *Journal of Construction Engineering and Management*, *135*(12), 1348–1356. doi:10.1061/(ASCE)CO.1943-7862.0000106

Glaser, T., & Pallas, F. (2007). *Information security and knowledge management: Solutions through analogies?* Rochester, NY: SSRN eLibrary.

Hatchimonji, G. (2013). Report indicates insider threats leading cause of data breaches in last 12 months, *CSO Online*. Retrieved from http://www.csoonline.com/article/2134056/network-security/report-indicates-insider-threats-leading-cause-of-data-breaches-in-last-12-months.html

He, W., Yuan, X., & Yang, L. (2013). Supporting case-based learning in information security with web-based technology. *Journal of Information Systems Education*, *24*(1), 31–40.

Jasimuddin, S. M., & Zhang, Z. J. (2013). Knowledge management strategy and organizational culture. *Journal of the Operational Research Society* Published online 04 September 2013 doi:10.1057jors.2013.101.

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, *9*(5), 493–504. doi:10.1007/s10796-007-9053-4

Kesar, S. (2008). Knowledge management within information security; the case of Barings Bank. *International Journal of Business Information Systems*, *3*(6), 652–667. doi:10.1504/IJBIS.2008.018996

Kesh, S., & Ratnasingam, P. (2007). A knowledge architecture for IT security. *Communications of the ACM*, *50*(7), 103–108. doi:10.1145/1272516

Leidner, D., Alavi, M., & Kayworth, T. (2006). The role of culture in knowledge management: A case study of two global firms. *International Journal of E-Collaboration*, *2*(1), 17–40. doi:10.4018/IJeC

Lemken, B., Kahler, H., & Rittenbruch, M. (2000). *Sustained knowledge management by organizational culture*. Proceedings of the 33rd Annual Hawaii International Conference on Issue Date: 4-7 Jan. 2000, Maui, Hawaii, On page(s): 10 pp. vol.2.

Lupiana, D. (2008). Development of a framework to leverage knowledge management systems to improve security awareness, *Dissertations. Paper 6*, Retrieved from http://arrow.dit.ie/scschcomdis/6

Maryam, A., Kayworth, T. R., & Leidner, D. E. (2005). An empirical examination of the influence of organizational culture on knowledge management practices. *Journal of Management Information Systems*, *22*(3), 191–224.

Mejias, R. J., & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security*, *10*(4), 160–185. doi:10.1080/15536548.2014.974407

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. (2011). When hackers talk: Managing information security under variable attack rates and knowledge dissemination. *Information Systems Research*, *22*(3), 606–623. doi:10.1287/isre.1100.0341

Park, H., Ribiere, V., & Schulte-Jr, W. D. (2004). Critical attributes of organizational culture that promote knowledge management technology implementation success. *Journal of Knowledge Management*, *8*, 106–117. doi:10.1108/13673270410541079

Parks, R. F., & Wigand, R. T. (2014). Organizational privacy strategy: Four quadrants of strategic responses to information privacy and security threats. *Journal of Information Privacy and Security*, *10*(4), 203–224. doi:10.1080/15536548.2014.974435

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(3), 757–778.

Roman, J. (2014). School breach affects 10,000, *Data Breach Today*, Retrieved from http://www.databreachtoday.com/school-breach-affects-10000-a-7033

Ting, C., Woon, I., & Kankanhalli, A. (2005). *Impact of security measures on the usefulness of knowledge management systems*, Pacific Asia Conference on Information Systems (PACIS) PACIS 2005 Proceedings, Bangkok, Thailand.

Wilson, T. (2014). Majority of users have not received security awareness training, study says, *Information Week Dark Reading*. Retrieved from http://www.darkreading.com/majority-of-users-have-not-received-security-awareness-training-study-says/d/d-id/1204329?

Downloaded by [University of New England] at 02:50 15 March 2016

المنارة للاستشارات

www.m

APPENDIX

A. Proof of Proposition 1

Proof: The firm's OLSA in the time period i can be rewritten as:

$$S_i = q(1-p_i)(1-rS_0)S_{i-1} + [1-q+qr(1-p_i)]S_0 + qp_i,$$

whose first-order derivative with respect to r is:

$$\frac{\partial S_i}{\partial r} = q(1-p_i)S_0(1-S_{i-1}) + q(1-p_i)(1-rS_0)\frac{\partial S_{i-1}}{\partial r} > 0.$$

The first-order derivative of OLSA S_i with respect to p_i is:

$$\frac{\partial S_i}{\partial p_i} = q(1-rS_0)(1-S_{i-1}) > 0.$$

when $p_i = 1$, $S_i(p_i = 1) = (1-q)S_0 + q > S_0$ and when $p_i = 0$,
$S_i(p_i = 0) = S_0 + q(S_{i-1} - S_0) + qrS_0(1-S_{i-1})$. Using this equation, when $i = 1$,
$S_1(p_1 = 0) = S_0 + qrS_0(1-S_0) > S_0$; when $i = 2$,
$S_2(p_2 = 0) = S_0 + q(S_1 - S_0) + qrS_0(1-S_1) > S_0, \ldots,$ when $i = n$,
$S_n(p_n = 0) = S_0 + q(S_{n-1} - S_0) + qrS_0(1-S_{n-1}) > S_0$. Therefore, $\forall i = 1, ..., n$,
$S_i > S_0$.
Hence, the first-order derivative of OLSA S_i with respect to q is:

$$\begin{aligned}\frac{\partial S_i}{\partial q} &= (1-p_i)(1-rS_0)S_{i-1} - [1-r(1-p_i)]S_0 + p_i \\ &= (1-p_i)S_{i-1} - (1-p_i)rS_0S_{i-1} - S_0 + r(1-p_i)S_0 + p_i \\ &= S_{i-1} - S_0 + r(1-p_i)S_0(1-S_{i-1}) + p_i(1-S_{i-1}) + q(1-p_i)(1-rS_0)\frac{\partial S_{i-1}}{\partial q} > 0.\end{aligned}$$

B. Proof of Proposition 2

Proof: Based on the firm's OLSA in a time period i, the highest OLSA is $S_i(p_i = 1)$ and the lowest OLSA is $S_i(p_i = 0)$; their difference is $S_i(p_i = 1) - S_i(p_i = 0) = q(1-rS_0)(1-S_{i-1})$.

C. Proof of Proposition 3

Proof: When the KMPQ in each period are the same (i.e., $p_i = p$), the firm's OLSA in each period can be derived from Equation (2) as

$$S_i = \frac{B}{1-A} + (S_0 - \frac{B}{1-A})A^i, \forall i = 1, 2, , n,$$

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

in which:

$$A = q(1-p)(1-rS_0),$$

$$B = [1-q+qr(1-p)]S_0 + qp.$$

when the total number of time periods goes to infinity,

$$S_\infty = \frac{[1-q+qr(1-p)]S_0 + qp}{1-q(1-p)(1-rS_0)}.$$

The first-order derivative of S_∞ with respect to p is:

$$\frac{\partial S_\infty}{\partial p} = \frac{q(1-rS_0)(1-q)(1-S_0)}{(1-A)^2} > 0.$$

The first-order derivative of S_∞ with respect to S_0 is:

$$\frac{\partial S_\infty}{\partial p} = \frac{qr(1-p)(1-q)(1-S_0)}{(1-A)^2} > 0.$$

The first-order derivative of S_∞ with respect to r is:

$$\frac{\partial S_\infty}{\partial p} = \frac{qS_0(1-p)(1-q)(1-S_0)}{(1-A)^2} > 0.$$

The first-order derivative of S_∞ with respect to q is:

$$\frac{\partial S_\infty}{\partial p} = \frac{S_0(1-r)+p(1-rS_0)+S_0(1-p)(1-rS_0)}{(1-A)^2} > 0.$$

D. Proof of Proposition 4

Proof: The firm's decision problem [P] for the base model can be rewritten as:

$$\max_{p_i} \ \pi = \sum_{i=1}^{n} \beta^{i-1}\{(O_L - w) + [S_{i-1} + (1-S_{i-1})p_i]q\Delta + L_i(S_0\Delta - \lambda)\},$$

where

$$L_i = 1 - q + (1-S_{i-1})(1-p_i)qr.$$

The firm's payoff in each period is:

$$\pi_i = O_L - w + C_i S_{i-1} + D_i,$$

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

where

$$C_i = q(1-p_i)[\Delta - S_0\Delta r + r\lambda],$$

$$D_i = p_i q\Delta + [1 - q + (1-p_i)qr](S_0\Delta - \lambda).$$

The first-order derivative of π_i with respect to p_i shows that

$$\frac{\partial \pi_i}{\partial p_i} = \frac{\partial C_i}{\partial p_i} S_{i-1} + \frac{\partial D_i}{\partial p_i}$$

$$= q[\Delta - S_0\Delta r + r\lambda](1 - S_{i-1}) > 0.$$

when $p_i = 1$, $\pi_i = O_L - w + q\Delta + (1-q)(S_0\Delta - \lambda)$. Therefore, when $O_L - w + q\Delta + (1-q)(S_0\Delta - \lambda) \geq 0$, or

$$\lambda > S_0\Delta + \frac{O_L - w + q\Delta}{1-q},$$

the firm should choose a KMRP in each period as high as possible.

E. Proof of Proposition 5

Proof: The firm's decision problem in this case can be rewritten as:

$$\max_{p_i} \ \pi = \sum_{i=1}^{n} \beta^{i-1}\{(O_L - w) + S_i\Delta - \theta L_i^{\theta}\},$$

where

$$L_i^{\theta} = (1 - S_{i-1})(1-p_i)(1-q).$$

The firm's payoff in each period is:

$$\pi_i = O_L - w + C_i^{\theta} S_{i-1} + D_i^{\theta},$$

where

$$C_i^{\theta} = (1-p_i)[q\Delta(1 - rS_0) + \theta(1-q)],$$

$$D_i^{\theta} = p_i q\Delta + [1 - q + (1-p_i)qr]S_0\Delta - \theta(1-p_i)(1-q).$$

The first-order derivative of π_i with respect to p_i shows that

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

$$\frac{\partial \pi_i}{\partial p_i} = \frac{\partial C_i^{\theta}}{\partial p_i} S_{i-1} + \frac{\partial D_i^{\theta}}{\partial p_i}$$
$$= [q\Delta(1 - rS_0) + \theta(1 - q)](1 - S_{i-1}) > 0.$$

when $p_i = 1$, $\pi_i = O_L - w + q\Delta + (1 - q)S_0\Delta > 0$. Therefore, the firm should choose a KMRP in each period as high as possible.

F. Proof of Proposition 6

Proof: The firm's decision problem in this case can be rewritten as:

$$\max_{p_i} \ \pi = \sum_{i=1}^{n} \beta^{i-1}\{(O_L - w) + S_i\Delta - \delta L_i^{\delta}\},$$

where

$$L_i^{\delta} = (1 - S_{i-1})(1 - p_i)qr.$$

The firm's payoff in each period is:

$$\pi_i = O_L - w + C_i^{\delta} S_{i-1} + D_i^{\delta},$$

where

$$C_i^{\delta} = (1 - p_i)[q\Delta(1 - rS_0) + \delta qr],$$

$$D_i^{\delta} = p_i q\Delta + [1 - q + (1 - p_i)qr]S_0\Delta - \delta(1 - p_i)qr.$$

The first-order derivative of π_i with respect to p_i shows that

$$\frac{\partial \pi_i}{\partial p_i} = \frac{\partial C_i^{\delta}}{\partial p_i} S_{i-1} + \frac{\partial D_i^{\delta}}{\partial p_i}$$
$$= [q\Delta(1 - rS_0) + \delta qr](1 - S_{i-1}) > 0.$$

when $p_i = 1$, $\pi_i = O_L - w + q\Delta + (1 - q)S_0\Delta$. Therefore, the firm should choose a KMRP in each period as high as possible.

G. Proof of Proposition 7

Proof: The firm's decision problem in this case can be rewritten as:

$$\max_{p_i} \ \pi = \sum_{i=1}^{n} \beta^{i-1}\{(O_L - w) + S_i\Delta - \varphi L_i^{\varphi}\},$$

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

where

$$L_i^{\varphi} = [S_{i-1} + (1 - S_{i-1})p_i](1 - q).$$

The firm's payoff in each period is:

$$\pi_i = O_L - w + C_i^{\varphi} S_{i-1} + D_i^{\varphi},$$

where

$$C_i^{\varphi} = (1 - p_i)[q\Delta(1 - rS_0) - \varphi(1 - q)],$$

$$D_i^{\varphi} = p_i q\Delta + [1 - q + (1 - p_i)qr]S_0\Delta - \varphi p_i(1 - q).$$

The first-order derivative of π_i with respect to p_i shows that

$$\frac{\partial \pi_i}{\partial p_i} = \frac{\partial C_i^{\varphi}}{\partial p_i} S_{i-1} + \frac{\partial D_i^{\varphi}}{\partial p_i}$$

$$= [q\Delta(1 - rS_0) - \varphi(1 - q)](1 - S_{i-1}) > 0,$$

if

$$\varphi < q\Delta(1 - rS_0)/(1 - q).$$

When $p_i = 1$, $\pi_i = O_L - w + q\Delta + (1 - q)S_0\Delta - \varphi(1 - q) > 0$ if $\varphi < q\Delta(1 - rS_0)/(1 - q)$. Therefore, the firm should choose a KMRP in each period as high as possible when $\varphi < q\Delta(1 - rS_0)/(1 - q)$.

H. Proof of Proposition 8

Proof: Following on the discussion in § 1, when the total number of time periods goes to infinity, the firm's OLSA in each period can be represented as:

$$S_i = \frac{B}{1 - A} + (S_0 - \frac{B}{1 - A})A^i, \forall i = 1, 2, , n,$$

in which

$$A = q(1 - p)(1 - rS_0),$$

$$B = [1 - q + qr(1 - p)]S_0 + qp.$$

Therefore, the firm's decision problem can be simplified as:

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

$$\max_{p} \quad \pi = \sum_{i=1}^{n} \beta^{i-1}\{(O_L - w) + [S_{i-1} + (1 - S_{i-1})p]q\Delta + L_i(S_0\Delta - \lambda)\},$$

where

$$L_i = 1 - q + (1 - S_{i-1})(1 - p_i)qr.$$

The firm's payoff in each period is:

$$\pi_i = O_L - w + CS_{i-1} + D,$$

where

$$C = q(1 - p)[\Delta - S_0\Delta r + r\lambda],$$

$$D = pq\Delta + [1 - q + (1 - p)qr](S_0\Delta - \lambda).$$

when the number of time periods goes to infinity, the firm's total payoff is:

$$\pi_\infty = \frac{1}{1-\beta} \cdot \left[O_L - w + \frac{C \cdot B}{1 - A} + D\right] + C \cdot \left[S_0 - \frac{B}{1 - A}\right] \cdot \frac{1}{1 - \beta A}$$

$$= \frac{O_L - w + D}{1 - \beta} + \frac{C \cdot S_0}{1 - \beta A} + \frac{C \cdot \beta \cdot B}{(1 - \beta A)(1 - \beta)}$$

The first order directive of π_∞ shows that:

$$\frac{\partial \pi_\infty}{\partial p} = \frac{\frac{\partial D}{\partial p}}{1 - \beta} + \frac{\frac{\partial C}{\partial p} S_0(1 - \beta A) + \beta C S_0 \frac{\partial A}{\partial p}}{(1 - \beta A)^2} + \frac{\beta}{1 - \beta} \cdot \frac{(C\frac{\partial B}{\partial p} + B\frac{\partial C}{\partial p})(1 - \beta A) + \beta CB\frac{\partial A}{\partial p}}{(1 - \beta A)^2},$$

where

$$\frac{\partial A}{\partial p} = -q(1 - rS_0),$$

$$\frac{\partial B}{\partial p} = -qrS_0 + q,$$

$$\frac{\partial C}{\partial p} = -q[\Delta - S_0\Delta r + r\lambda], \textit{and}$$

$$\frac{\partial D}{\partial p} = q\Delta - qr(S_0\Delta - \lambda).$$

Simplifying the first order directive of π_∞ follows that:

Downloaded by [University of New England] at 02:50 15 March 2016

www.m

$$\frac{\partial \pi_\infty}{\partial p} = \frac{q(\Delta - S_0 \Delta r + r\lambda)}{(1-\beta)(1-\beta A)^2} \cdot [(1-S_0)(1-\beta q) + (\beta A)^2] \geq 0.$$

Therefore, the optimal homogeneous KMPQ p^* should be as high as possible, i.e., $p^* = 1$, for which the firm's total payoff is:

$$\pi_\infty^* = \frac{O_L - w + q\Delta + (1-q)(S_0\Delta - \lambda)}{1-\beta}.$$

Finally, it was concluded that the above solution that $p^* = 1$ is valid only when $\pi_\infty^* \geq 0$, or

$$\lambda > S_0 \Delta + \frac{O_L - w + q\Delta}{1-q}.$$

The proof for the other parts of the proposition is similar as that for the part shown here.

Downloaded by [University of New England] at 02:50 15 March 2016

www.m