**Association for Information Systems**
**AIS Electronic Library (AISeL)**

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

# Managing Information Security via Transactive Memory Systems: An IT-HR Collaboration Perspective

Kamphol Wipawayangkool
*The University of Texas at Arlington*, kamphol.wipawayangkool@mavs.uta.edu

# Managing Information Security via Transactive Memory Systems: An IT-HR Collaboration Perspective

**Kamphol Wipawayangkool**
The University of Texas at Arlington
kamphol.wipawayangkool@mavs.uta.edu

## ABSTRACT

Human factors are increasingly recognized as real culprits of failures in Information Security Management (ISM). Thus, the roles of Human Resource Management (HRM) become more salient with ISM. Unlike practitioners, researchers appear reluctant to acknowledge such emergence. Prior literature has not attempted to link ISM with HRM theoretically. ISM literature suggests that both technical and non-technical aspects be simultaneously considered. Similarly, HRM literature recommends that practices such as staffing and training be treated as a bundle. Evidently, both ISM and HRM teams require a pool of specialized knowledge and skills to manage each of their aspects. Moreover, both teams should collaborate in order to improve the ISM performance of the firm. However, the amount of the knowledge may become overloading to both teams. This paper posits that Transactive Memory System (TMS) can support not only knowledge coordination when each team operates independently, but also alleviate the knowledge overload when both teams collaborate. Furthermore, this paper proposes that such collaboration via TMS enables an organization to not only manage its ISM more effectively but ultimately produce sustainable competitive advantage. Implications are then discussed.

**Keywords**
Information security, human resources, transactive memory systems, collaboration, sustainable competitive advantage.

## INTRODUCTION

Both practitioners and researchers increasingly acknowledge that the real culprits of failures in Information Security Management (ISM) are human behaviors rather than technology. The 2007 Deloitte Global Security Survey (DGSS) with respondents from 169 major global financial institutions reported that compared to prior years, improvements to technical infrastructure did not make the top priorities, but non-technological factors such as access and identity management (50%), security regulation and compliance (49%), and security training and awareness (48%) were the top three priorities. Throughout the survey, the discussion made clear that information security is no longer a technology-focused issue. Similarly, the 10$^{th}$ annual Ernst & Young Global Information Security Survey (EYGISS) (2007) with nearly 1300 organizations from such industries as financial services, manufacturing, technology, health services, and government, showed that compliance and regulations (64%), privacy and data protection (58%), and aligning information security with business objectives (45%) were the top three drivers that most significantly affect ISM of the organization, while technology-related drivers (less than 15%) were not even in the top five. Taken together, these two global surveys clearly show that practitioners have realized the greater implications of non-technical activities. Likewise, researchers recently acknowledge that managing human-related factors such as awareness (Choi et al., 2006; Dhillon, 2007; Schultz, 2004; Siponen, 2000; von Solms, 2001; von Solms, 2006) and culture (Chang and Lin, 2007; Ruighaver et al., 2007; von Solms and von Solms, 2004; Vroom and von Solms, 2004) appears to be critical and fundamental to all aspects of ISM and are more challenging than merely managing technology.

As people factors are more profoundly significant than technology factors, the role of Human Resource Management (HRM) unavoidably becomes salient with ISM. Again, the discussion in the 2007 DGSS (p. 11) elaborated how people remain the weakest link in ISM. First, as the top priority, information access and identity management imply that how an organization screens and employs people is crucial, that simple criminal background checks are not enough, and that the impact of possible abuses must be expectedly determined. Second, in addition to staffing issues, security training ranks third in the top five. Recognizing that how people deal with information represents either intentional or unintentional risks, the organization should provide security training and awareness programs that are tailored to targeted groups (p. 14). Importantly, the outcomes of such programs must be measured to determine whether the participants have learned and acquired the knowledge. Similarly, the 2007 EYGISS suggests that staffing and training are pivotal to successful ISM (p. 17). As organizations are now more focused on regulations and compliances, the challenges in staffing experienced and well-trained people to practice ISM become multifold in addition to day-to-day security knowledge and skills. The lack of skilled human

resources is far more critical than that of technological resources. Thus, finding the right human resources inside and outside of the organization is becoming one of the greatest challenges in ISM. The survey also shows that finding internal resources is far more difficult than finding external resources (p. 18). The survey concludes the staffing issues by suggesting that staffing models will change in the future as the gaps of security-related staff increase, for example non-IT staff may fill those gaps as well as third-party organizations.

Both ISM and HRM have their own aspects and practices. Researchers suggest that both technical and non-technical aspects should be considered simultaneously. Similarly, researchers suggest that HRM practices such as staffing and training should be treated as a bundled system (Barney and Wright, 1998; Pfeffer, 2005; Wright and McMahan, 1992; Wright et al., 1994). One should not assume that an experienced security (or human resource) professional will be the expert of all practices in all of the aspects. In addition to operating independently, both ISM and HRM teams should collaborate in order to improve the ISM performance of the firm. However, given many aspects of both ISM and HRM, the amount of specialized knowledge may become too much to be executed strategically. Thus, an appropriate collaboration mechanism is needed in order to improve the ISM performance of the firm. This paper posits that Transactive Memory System (TMS) as a knowledge coordination mechanism can support not only knowledge coordination when each team operates independently in its realm, but also alleviate the knowledge overloading when both teams collaborate. Furthermore, this paper proposes that the collaboration between ISM and HRM teams via TMS enables an organization to not only manage its ISM more effectively but ultimately produce sustainable competitive advantage.

This paper is organized as follows. First, literature background on ISM and HRM is presented. Second, how staffing and training become involved with ISM and how they can help improve the ISM performance of the firm are discussed. Third, literature background on TMS and how it can support the collaboration between ISM and HRM teams are discussed as well as research model and propositions. Finally, future studies are discussed as well as both theoretical and practical implications.

## LITERATURE BACKGROUND AND RESEARCH MODEL DEVELOPMENT

### Information Security Management

Classically, the core principles of Information Security Management (ISM) are confidentiality (to ensure privacy of information), integrity (to ensure authorized operations on information), and availability (to ensure availability of functional systems) (Dhillon, 2007). Both technical and non-technical aspects exist throughout those ISM principles. *Technical* aspects include computer software and hardware control concepts such as encryption and network security (Dhillon, 2007). Although behavioral factors are more influential to successful ISM as previously discussed, technology still needs to be updated to provide fundamental protections to corporate networks. One infamous case (and many more retailers) is T.J. Maxx in which its wireless networks were not updated to be equipped with superior encryption mechanisms (i.e. using WEP instead of WPA or WPA2), leading to its data breach (Greenemeier, 2007).

Non-technical aspects cover topics such as management and regulatory compliance. *Managerial* aspects essentially include risk management, corporate governance, and culture management (Dhillon, 2007; Nosworthy, 2000; von Solms, 2000, 2001, 2006). Risk analysis has become a standard practice used to forecast and evaluate financial benefits of the investments proposed to counter predicted risks (Dhillon and Backhouse, 2001). Corporate governance covers such managerial activities as developing security policies, improving people's awareness (Choi et al., 2006; Jones, 2007; Kelly, 2006; Siponen, 2000; von Solms, 2001), and building security culture. Organizational culture is crucial as it helps ensure that policies are appropriately manifested in people's behaviors. Finally, *regulatory* aspects refer to compliances with laws and regulations. International security standards such as ISO/IEC 27001 and 27002 (previously ISO/IEC 17799) become more relevant to many modern organizations as they operate across countries. The ISO/IEC 27001 and 27002 explicitly indicate that people, process, and information are as critical factors in ISM as technology. Both of the standards include controls in security policy, organizing information security, asset management, human resources security, physical and environmental security, communication and operations management, access control, information systems acquisition, development, and maintenance, incident management, business continuity management, and compliance (Humphreys, 2008).

In summary, both technical and non-technical aspects of ISM must be effectively managed to achieve and maintain the core principles of ISM. Given the complexity of each of the aspects as discussed above, an organization definitely needs a large pool of specialized knowledge and skills in both technical and managerial areas. Having IT staff does not translate to having security staff. Since people factors are significantly omnipresent in all aspects of ISM as discussed above, it is only reasonable to acknowledge the roles of human resource management. Thus, the roles of human resource management are discussed next.

### The Role of Human Resource Management

Human Resource Management (HRM) refers to the uses of practices such as staffing, training, appraisal, and rewards to manage people in organizations (Fombrum et al., 1984). Researchers increasingly suggest that those practices should be strategically integrated so that an organization can effectively utilize its human resources to achieve its strategic goals and ultimately to produce sustainable competitive advantage (Barney and Wright, 1998; Pfeffer, 2005; Wright and McMahan, 1992; Wright et al., 1994). Empirical evidence also supports such view. For example, Ichniowski et al. (1997) found that a combination of effective HR practices substantially improves productivity. Huselid (1995) found that the complementarities among HR practices not only reduce employee turnover but also increase productivity and corporate financial performance. Macduffie (1995) found that plants that bundled HR practices with business strategy significantly perform better in both productivity and quality. Therefore, this paper posits that if effective HR practices such as staffing and training are strategically bundled together with security policies, an organization will be able to manage its ISM more effectively and ultimately produce its sustainable competitive advantage. Based on existing literature, this paper next elaborates particularly how both staffing and training are instrumental to successful ISM.

Regardless of the pervasiveness of non-technical factors in ISM, it is fair to say that not every non-technical factor is equally important. Both researchers and practitioners suggest that insider threats (Humphreys, 2008; Theohariduo et al., 2005) and security awareness (Choi et al., 2006; Jones, 2007; Kelly, 2006; Siponen, 2000; Straub and Welke, 1998; von Solms and von Solms, 2004; von Solms, 2001) are among greatest risks in security arena. First, insider threats refer to threats originating from people who can access to the corporate systems and abuse such privileges for personal gains. Such misbehaviors violate security protection of the firm and lead to losses of a combination of tangible and intangible assets. Second, according to the Information Security Forum (ISF) (2005), security awareness is defined as the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. Many incidents of security breaches occur simply because people lack security awareness. The ISO/IEC 27001 and 27002 (previously ISO/IEC 17799), as mentioned in ISM section, explicitly includes human resource security as one of the controls (Humphreys, 2008; Theohariduo et al., 2005). The section points out that HR department should have well-defined procedures as follows. First, during recruitment, processes such as including security in job responsibilities, conducting background and reference checking should be carefully executed. Furthermore, qualifications of the candidates should really meet the required knowledge, abilities, and skills. Second, during employment, employers should require employees to sign confidentiality agreement, and should offer effective security awareness and training programs. In addition, individuals in privileged positions should be regularly checked to ensure their appropriate right and level of information access. Finally, at the termination of employment, employers should remove all associated computer accounts from the systems. Again, to emphasize the acknowledgment among practitioners, the aforementioned two global surveys suggest both directly and indirectly that both staffing and training are very critical to effective ISM. Thus, the question “how can HR team collaborate with IT team to manage ISM effectively?” is explored next as well as the issues of knowledge overload that is likely to occur during the collaboration.

### The Issue of Knowledge Overload

Information overload refers to the condition in which the amount of information available is greater than the ability of individuals to process (Ireland, 1999; O’Reilly, 1980). From this point on, this paper uses the term knowledge overload to mainly refer to the key information especially pertinent to ISM and to reflect the significance and difficulty of ISM in organization nowadays. Kock (2000) found that as interactions increase, processing efficiency decreases, ultimately constituting the condition of knowledge overload. Considering both technical aspects of ISM IT team has to confront and non-technical aspects of ISM HR team should be able to support, it is fairly reasonable to establish that either team can face the issues of knowledge overload. The first situation is when either team independently works in its field. Considering such technical aspects of ISM as encryption, hardware controls, software controls, and network security, an experienced staff in one area should not be mistaken to also be an expert in another. IT staff has to interact among each other in order to ensure the security principles (confidentiality, integrity, and availability) of all systems. Under circumstances, team members may become overwhelmed and unsure whom to contact for certain knowledge and skills. Similarly, one staff experienced in practicing staffing employees should not be assumed to also be experienced in designing training programs. Specifically to ISM, HR staff has to ensure that non-technical aspects, such as selecting security staff and offering security training, are effectively managed to help achieve the goals of ISM. Furthermore, when the common goal of both teams is the principles of ISM, it is unavoidable that both teams have to collaborate to each other. Kock (2000) found that types of knowledge and skills also affect the processing ability. In other words, HR team may not be able to process knowledge coming from IT team and vice versa. Therefore, the IT-HR collaboration is likely to exponentially increase the amount of knowledge overload; consequently, the ISM goals are unlikely to be achieved, if at all, in effective and efficient manners.

### The IT-HR Collaboration via Transactive Memory Systems

Researchers find that the concept of transactive memory not only helps knowledge-intensive project teams manage their members' knowledge and expertise and match people with appropriate skills, but also helps maintain effective interactions among members, a combination which ultimately improves team performance (Akgun et al., 2005; Kanawattanachai and Yoo, 2007; Lewis, 2004). To ease the transition to the discussion from this section on, both IT and HR are considered two different teams. In addition, this paper assumes that focal to both teams is ISM, a grand ongoing strategic project of a firm that includes smaller projects requiring both continuous and intermittent interactions between both teams.

Wegner (1986) conceptualized a Transactive Memory System (TMS) as a combination of both a set of individuals' memories and the interactions among the individuals in the team to store and retrieve one another's specialized knowledge. The underlying concept is that with limited memory and knowledge, individuals can use other people's memories as additional knowledge storage by knowing "*who knows what*" rather than having to possess actual knowledge themselves. As a result, TMS facilitates knowledge coordination by providing team members more efficient access to larger and more complex repositories of individuals' specialized knowledge than each individual's own memory system (Akgun et al., 2005; Lewis, 2004; Wegner, 1986). In other words, TMS helps reduce knowledge overload flowing among teams. TMS typically comprises three dimensions: specialization, credibility, and coordination (Lewis 2003). *Specialization* exists because team members possess specialized knowledge from different domains. *Credibility* allows team members to believe that they can rely on others' knowledge and that others will provide their knowledge into the TMS as needed. *Coordination* among team members occur when they know who has what knowledge and understand how that knowledge can support their tasks. Taken together, TMS reflects both cognitive (specialization and credibility) and behavioral state (coordination) (Ellis 2006). Thus, it can be said that TMS helps team members manage their knowledge coordination better because they can manage their mental processes and behaviors more effectively and efficiently.

Originally, Wegner (1986) posited that TMS exists in teams whose members have closer relationship. As a result, a legitimate question is "can TMS exist at this interdepartmental collaboration between IT and HR team?" This paper answers such a question by drawing an analogy between the nature of this IT-HR collaboration and the collaboration in virtual teams as follows. Virtual teams are defined as teams whose members are geographically dispersed, interdependent on their tasks yet share responsibility for outcomes, and rely on technology-mediated communications rather than face-to-face interaction to accomplish the tasks (Aubert and Kelsey, 2003; Jarvenpaa and Leidner, 1999; Powell et al., 2004; Schiller and Mandviwalla, 2007). Additionally, team members can come from different organizations (Aubert and Kelsey, 2003) and typically are formed temporarily to accomplish specific goals (Powell et al. 2004). While virtual teams offer advantages over traditional face-to-face teams in terms of overcoming geography, time, and organization boundaries, researchers concur that team communication and coordination processes are so critical that they significantly affect team performance (Espinosa et al., 2007; Martins et al., 2004; Powell et al., 2004). Therefore, the nature of virtual environments obviously challenges how virtual team members coordinate their knowledge (Espinosa et al., 2007; Sarker et al., 2002) much more than do face-to-face teams. Indeed, Espinosa et al. (2007) found that geographic distance has a negative effect on coordination, but is mitigated by shared knowledge of the team and awareness of the expertise presence. Thus, in short, it is reasonable to infer that the collaboration challenges between IT and HR team should appear to be fairly similar to those of virtual teams (i.e. members with unique and different expertise in different locations with sparse physical contacts yet attempting to achieve the common goals of ISM). In other words, how IT and HR teams collaborate in ISM should be similar to how virtual teams' members generally work together (less physically and more electronically), since the notion of virtual teams does not suggest complete elimination of physical interactions but merely limited. Kanawattanachai and Yoo (2007) found that although taking relatively long time to develop, virtual teams can form TMS. They found that the frequency and volume of task-oriented communication are significant in forming TMS in early phases, while task-knowledge coordination is in later phases. Importantly, they found that TMS enables virtual teams to perform more effectively.

Therefore, this paper posits that given time, TMS between IT and HR teams can emerge and have effects in similar fashions to TMS in virtual teams. Specifically, given time and interaction, the TMS of IT team should grow and help reduce the knowledge overload when people exchange knowledge across different technical aspects. As a result, the IT TMS should help improve the ISM performance of the firm (e.g. fewer incidents and improved effectiveness of prevention mechanisms). Likewise, the TMS of HR team should be established and help reduce the knowledge overload when staff from different HR practices interacts with each other. As a result, the HR TMS should also help improve the ISM performance of the firm (e.g. mitigated insider threats and increased level of security awareness). More importantly, when both teams have to collaborate, as discussed earlier, the knowledge overload is likely to increase exponentially. Therefore, if IT team has access to the HR TMS and vice versa, the collective TMS should reduce the knowledge overload in a similar manner. As a result, such collaboration will improve the ISM performance of the firm. Taken together, the propositions are developed as follows:

*Proposition 1: Once established, the TMS of IT team will help reduce the degree of knowledge overload occurring from the collaboration among the team members with different knowledge pertinent to different technological aspects of ISM. As a result, IT team will be able to manage and utilize its pool of knowledge better. Ultimately, the collaboration within IT team via its TMS will improve the ISM performance of the firm.*

*Proposition 2: Once established, the TMS of HR team will help reduce the degree of knowledge overload occurring from the collaboration among the team members with different knowledge pertinent to different non-technological aspects of ISM. As a result, HR team will be able to manage and utilize its pool of knowledge better. Ultimately, the collaboration within HR team via its TMS will improve the ISM performance of the firm.*

*Proposition 3: In addition to the existence of independent TMS in both IT and HR teams, the collective TMS occurring when one team has access to the other's TMS and vice versa will reduce the degree of knowledge overload exponentially. Ultimately, the collaboration between IT and HR team via the collective TMS will improve the ISM performance of the firm.*

### Linking to Sustainable Competitive Advantage

This paper not only proposes that the collaboration between IT and HR team can improve the ISM performance of the firm, but also that such collaboration can ultimately produce sustainable competitive advantage. To justify such position, this paper draws from Barney (1991)'s Resource-Based View of the firm (RBV). In the RBV framework, four factors that determine the potential of the firm resources to produce sustained competitive advantage are value, rareness, inimitability, and non-substitutability. This paper mainly adopts the definitions of the following variables from Barney's work (1991). *Firm resources* include physical capital resources (e.g. technology), human capital resources (e.g. intelligence, experience, and relationships), and organizational capital resources (e.g. firm structure, management systems, and relations among departments). *Sustained competitive advantage* exists when a firm implements "a value creating strategy not simultaneously being implemented by any current or potential competitors and when these other firms are unable to duplicate the benefits of this strategy" (Barney 1991, p. 102). For firm resources to be able to produce sustained competitive advantage, they must provide *value* to the firm, must be *rare*, must be *inimitable*, and must be *non-substitutable*. To human resources, Wright and McMahan (1992) reviewed literature and found that there exist explicit formulae to quantify the values of human resources and that basically the values exist when employees have different knowledge and skills to contribute to the firm performance e.g. decreasing costs and increasing revenues (Barney and Wright, 1998). Second, they noted that human resources in fact fall under the normal distribution; thus, people with high ability are rare to find. Third, they discussed that organization's unique history, social relationships, and culture reflect the inimitability of human resources. A case in point is Southwest Airlines' uniquely dynamic culture that is well-known in the industry to contribute to the success of the company (Barney and Wright, 1998). Finally, to achieve the status of non-substitutability, the resources should be strategically exploited, indicating the importance of managing HR practices as a bundle (Barney and Wright, 1998; Wright and McMahan, 1992). If people are viewed independently as a resource, chances are technology may be able to replace them. In sum, researchers suggest that strategic use of human resources can produce sustained competitive advantage.

Based on the discussion above, this paper considers the collaboration between IT and HR teams a potential resource of the firm that can produce sustainable competitive advantage. To lay the foundation of the argument, this paper refers to Bhatt and Grover (2005)'s findings. They found that the quality of IT infrastructure is not associated with competitive advantage, but importantly 1) the ability of the firm to integrate IT strategy and business strategy and 2) the ability of the IT team to understand business needs and create a partnership with other business teams are found to be significantly associated with competitive advantage of the firm. In short, the effective strategic collaboration between IT teams and other business teams is likely to produce competitive advantage. Given that human resources are value, rare, inimitable, and more importantly non-substitutable if treated as a bundle, it is reasonable to infer that if the strategic HR bundle is effectively coupled with the IT strategy can become a potential resource to produce sustainable competitive advantage. Indeed, Barney and Wright (1998) suggested that sustainable competitive advantage rather comes from the notion of combination (i.e. from teams than individuals and from bundled than individual HR practices). As earlier discussed, since TMS can both support knowledge coordination and maintain relationships between the teams at both cognitive and behavioral levels conceivably leading to greater extent of rareness, inimitability, and non-substitutability, the entire strategy of IT-HR collaboration via TMS is even more likely to become a very potential resource to produce sustainable competitive advantage. In other words, the more effective the strategic collaboration between the teams is, the more the competitive advantage is likely to be sustainable.

*Proposition 4: The strategic collaboration between IT and HR team via TMS can produce sustainable competitive advantage.*

Below, Figure 1 depicting all four propositions represents the research model of the IT-HR collaboration via TMS.

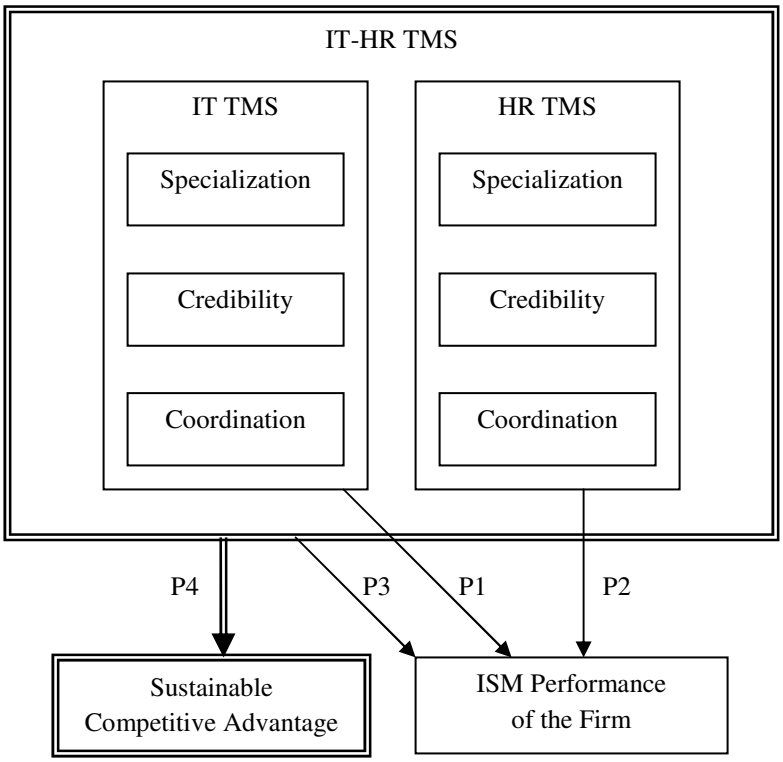


**Figure 1. Research Model: IT-HR Collaboration via TMS**

## IMPLICATIONS

Recognizing the significant of human factors in ISM, this paper contributes most to security literature as the link between ISM and HRM is theoretically established through multiple theories such as information overload, transactive memory system, and resource-based value of the firm. This theoretical integration opens a number of future directions on studying the strategic roles of HRM on ISM. First, empirical studies to support the propositions developed in this paper are needed. Second, the taxonomy of both IT TMS and HR TMS constructs needs to be developed particularly for ISM context. Third, the effects of the IT-HR collaboration via TMS on firms' sustainable competitive advantage should be definitely tested for many times before the conclusion can be made. It is important to recognize that other factors also play roles in producing sustainable competitive advantage. Barney (1991) noted that sustained competitive advantage does not suggest that it will last forever, because both organizational and environmental factors may shift such status at any time. As a result, to re-generate and test hypotheses based on the propositions above, the ultimate construct could be competitive advantage rather than sustainable competitive advantage to avoid the issue of temporal effects. Thus, whether such competitive advantage can actually be sustained should be explored further empirically and especially longitudinally.

For practitioners, the proposed benefits of the IT-HR collaboration should not be improbable at all. In fact, this paper is partly driven by practitioners' global survey findings. Practitioners should continue to increase their emphasis on the greater implications of non-technological factors. Staffing and training techniques should be seen as very instrumental to successful ISM; as a result, IT and HR should continuously collaborate although a certain security project, e.g. security awareness training, is over in order to learn, profile, and document the processes of staffing and training particularly for ISM. In other words, general practices of staffing and training should not be assumed to fit well with ISM policies. Bhatt and Grover (2005) suggested that higher level of organizational learning have positive effect on the competitive advantage of the firm. Thus, continuous learning from each other may help sustain competitive advantage of the firm to a certain degree. Although this paper explicitly links staffing and training as literature suggests they are instrumental to successful ISM, other HR practices such as compensation system are not any less important (e.g. pay may help maintain employees' organizational commitment

and satisfaction to minimize insiders' threats). In fact, as strategic HR researchers suggest, the more the HR practices are strategically bundled together with security policies, the better the ISM performance of the firm should be. Thus, this absence of other HR practices in this paper should definitely open myriad future directions to both security researchers and organizational researchers. Finally, although the TMS discussed in this paper is a conceptual construct, IT such as intranet and information directory should be considered and utilized to reduce information overload and to better support the collaboration among teams (Edmunds and Morris, 2000; Ireland, 1999). As a result, other factors such as IT infrastructure investment and IT capability may affect the benefits to be received from the collective IT-HR TMS to some extent that disadvantages such as a variety of costs are present. Nonetheless, once such an IT-based TMS is successfully implemented and well settled with all teams' members, the knowledge overloading as viewed as a key issue will be minimized and the advantages are expected in long term to be aligned with the propositions which are improving overall ISM performance and creating competitive advantage of the firm.

## CONCLUSION

Both researchers and practitioners increasingly acknowledge that human factors are real culprits of failures in Information Security Management (ISM). As a result, the roles of Human Resource Management (HRM) become more salient with the information security realm. Prior literature has not attempted to link ISM with HRM theoretically. Drawing from multiple theories, this paper proposes a theoretical framework of the IT-HR collaboration via Transactive Memory System (TMS). Specifically, TMS can support not only knowledge coordination when each team operates independently in its field but also reduce the knowledge overload when both teams collaborate. Ultimately, such collaboration is expected to enable an organization to not only improve its ISM performance but also produce sustainable competitive advantage.

## REFERENCES

1. Akgun, A.E., Byrne, J., Keskin, H., Lynn, G.S., and Imamoglu, S.Z. (2005) Knowledge networks in new product development projects: A transactive memory perspective, *Information & Management*, 42, 1105-1120.
2. Aubert, B.A. and Kelsey, B.L. (2003) Further understanding of trust and performance in virtual teams, *Small Group Research*, 34, 5, 575-618.
3. Barney, J. (1991) Firm resources and sustained competitive advantage, *Journal of Management*, 17, 1, 99-120.
4. Barney, J.B. and Wright, P.M. (1998) On becoming a strategic partner: the role of human resources in gaining competitive advantage, *Human Resource Management*, 37, 1, 31-46.
5. Bhatt, G.D. and Grover, V. (2005) Types of information technology capabilities and their role in competitive advantage: An empirical study, *Journal of Management Information Systems*, 22, 2, 253-277.
6. Bresz, F.P. (2004) People—often the weakest link in security, but one of the best places to start, *Journal of Health Care Compliance*, 57-60.
7. Chang, S.E. and Ho, C.B. (2006) Organizational factors to the effectiveness of implementing information security management, *Industrial Management & Data Systems*, 106, 3, 345-361.
8. Chang, S.E. and Lin, C. (2007) Exploring organizational culture for information security management, *Industrial Management & Data Systems*, 107, 3, 438-458.
9. Choi, N., Kim, D.J., and Goo, J. (2006) Managerial information security awareness' impact on an organization's information security performance, *Proceedings of the Twelfth Americas Conference on Information Systems*, 2006, 3367-3375.
10. Dhillon, G. (2007) Principles of information systems security: Text and cases. John Wiley & Sons, Inc.
11. Dhillon, G. and Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives, *Information Systems Journal*, 11, 127-153.
12. Edmunds, A. and Morris, A. (2000) The problem of information overload in business organizations: A review of the literature, *International Journal of Information Management*, 20, 17-28.
13. Ellis, A.P.J. (2006) System breakdown: The role of mental models and transactive memory in the relationship between acute stress and team performance, *Academy of Management Journal*, 49, 3, 576-589.
14. Espinosa, J.A., Slaughter, S.A., Kraut, R.E., and Herbsleb, J.D. (2007) Team knowledge and coordination in geographically distributed software development, *Journal of Management Information Systems*, 24, 1, 135-169.
15. Fombrum, C., Tichy, N., and Devanna, M. (1984) Strategic human resource management. New York, Wiley.
16. Greenemeier, L. (2007) T.J. Maxx data theft likely due to wireless 'wardriving'. http://www.eetimes.com/showArticle.jhtml?articleID=199500574
17. Humphreys, E. (2008) Information security management standards: Compliance, governance, and risk management, *Information Security Technical Report*, doi: 10.1016/j.istr.2008.10.010

18. Huselid, M.A. (1995) The impact of human resource management practices on turnover, productivity, and corporate financial performance, *Academy of Management Journal*, 38, 3, 635-672.
19. Ichniowski, C., Shaw, K., and Prennushi, G. (1997) The effects of human resource management practices on productivity: A study of steel finishing lines, *The American Economic Review*, 87, 3, 291-313.
20. Ireland, P. (1999) Management paradigm to reduce information overload, *Computing & Control Engineering Journal*, February, 29-32.
21. Jahner, S. and Kremar, H. (2005) Beyond technical aspects of information security: Risk culture as a success factor for IT risk management, *Proceedings of the Eleventh Americas Conference on Information Systems*, 3327-3336.
22. Jarvenpaa, S.L. and Leidner, D.E. (1999) Communication and trust in global virtual teams, *Organization Science*, 10, 6, 791-815.
23. Jones, D. (2007) Low cost security tools: Employee awareness, *Security*, November, 90-91.
24. Kanawattanachai, P. and Yoo, Y. (2007) The impact of knowledge coordination on virtual team performance over time, *MIS Quarterly*, 31, 4, 783-808.
25. Kelly, C.J. (2006) Awareness trumps new security toys, *Computerworld*, October, 44.
26. Kock, N. (2000) Information overload and worker performance: A process-centered view, *Knowledge and Process Management*, 7, 4, 256-264.
27. Lewis, K. (2003) Measuring transactive memory systems in the field: Scale development and validation, *Journal of Applied Psychology*, 88, 4, 587-604.
28. Lewis, K. (2004) Knowledge and performance in knowledge-worker teams: A longitudinal study of transactive memory systems, *Management Science*, 50, 11, 1519-1533.
29. Macduffie, J.P. (1995) Human resource bundles and manufacturing performance: Organizational logic and flexible production systems in the world auto industry, *Industrial and Labor Relations Review*, 48, 2, 197-221.
30. Martins, L.L., Gilson, L.L., Maynard, M.T. (2004) Virtual teams: What do we know and where do we go from here? *Journal of Management*, 30, 6, 805-835.
31. Nosworthy, J.D. (2000) Implementing information security in the 21st century – Do you have the balancing factors? *Computers & Security*, 19, 337-347.
32. O'Reilly CA. (1980) Individuals and information overload in organizations: is more necessarily better? *Academy of Management Journal*, 23, 4, 684-696.
33. Pfeffer, J. (2005) Producing sustainable competitive advantage through the effective management of people, *Academy of Management Executive*, 19, 4, 95-106.
34. Powell, A., Piccoli, G., and Ives, B. (2004) Virtual teams: A review of current literature and directions for future research, *The DATA BASE for Advances in Information Systems*, 35, 1, 6-36.
35. Ruighaver, A.B., Maynard, S.B., and Chang, S. (2007) Organisational security culture: Extending the end-user perspective, *Computers & Security*, 26, 56-62.
36. Sarker, S., Sarker, S., Nicholson, D., and Joshi, K. (2002) Knowledge transfer in virtual information systems development teams: An empirical examination of key enablers, *Proceedings of the 36th Hawaii International Conference on System Sciences*.
37. Schiller, S.Z. and Mandviwalla, M. (2007) Virtual team research: An analysis of theory use and a framework for theory appropriation, *Small Group Research*, 38, 1, 12-59.
38. Schultz, E. (2004) Security training and awareness-fitting a square peg in a round hole, *Computers & Security*, 23, 1-2.
39. Schultz, E. (2004) Sarbanes-Oxley-a huge boon to information security in the US, *Computers & Security*, 23, 353-354.
40. Siponen, M.T. (2000) A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, 8, 1, 31-41.
41. Straub, D.W. and Welke, R.J. (1998) Coping with systems risk: Security planning models for management decision making, *MIS Quarterly*, December, 441-469.
42. Theohariduo, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2005) The insider threat to information systems and the effectiveness of ISO17799, *Computers & Security*, 24, 472-484.
43. Thomson, M.E. and Von Solms, R. (1998) Information security awareness: Educating your users effectively, *Information Management and Computer Security*, 6, 4, 167-173.
44. Von Solms, B. (2000) Information Security – The third wave? *Computers & Security*, 19, 615-620.
45. Von Solms, B. (2001) Information Security – A multidimensional discipline, *Computers & Security*, 20, 504-508.
46. Von Solms, B. (2006) Information Security – The fourth wave, *Computers & Security*, 25, 165-168.
47. Von Solms, B and Von Solms, R. (2004) The 10 deadly sins of information security management, *Computers & Security*, 23, 371-376.
48. Von Solms, R and Von Solms, B. (2004) From policies to culture, *Computers & Security*, 23, 275-279.

49. Vroom, C., and Von Solms, R. (2004) Towards information security behavioral compliance, *Computers & Security*, 23, 191-198.
50. Wegner, D. M. (1987) Transactive memory: A contemporary analysis of the group mind. In B. Mullen & G. R. Goethals (Eds.), Theories of group behavior (pp. 185–208). New York: Springer-Verlag.
51. Wright, P.M. and McMahan, G.C. (1992) Theoretical perspectives for strategic human resource management, *Journal of Management*, 18, 2, 295-320.
52. Wright, P.M., McMahan, G.C., and McWilliams A. (1994) Human resources and sustained competitive advantage: a resource-based perspective, *International Journal of Human Resource Management*, 5, 2, 301-326.