Exploring Knowledge Sharing Practices for Raising Security Awareness

Hiep-Cong Pham
School of Business and Management
RMIT University Vietnam
Ho Chi Minh City, Vietnam
Email: hiep.pham@rmit.edu.vn

Irfan Ulhaq
School of Business and Management
RMIT University Vietnam
Ho Chi Minh City, Vietnam
Email: irfan.ulhaq@rmit.edu.vn

Mathews Nkhoma
School of Business and Management
RMIT University Vietnam
Ho Chi Minh City, Vietnam
Email: mathews.nkhoma@rmit.edu.vn

Minh Nhat Nguyen
School of Business and Management
RMIT University Vietnam
Ho Chi Minh City, Vietnam
Email: minh.nguyennhat@rmit.edu.vn

Linda Brennan
School of Media & Communication
RMIT University Australia
Melbourne, Victoria, Australia
Email: linda.brennan@rmit.edu.au

Abstract

This study aims to explore the types of information can be effectively communicated in three knowledge-sharing methods and their impact on employees' security practice. On one end, guarding the organisation's information system against cyber-attacks is critical and improving users' knowledge and skills is a common approach to any security program. On the other end, organisations lack a clear understanding in determining what types of security information should be delivered through various methods of communication to be effective in boosting users' knowledge and compliance behaviour. The study employed a qualitative method using semi-structured interviews with business users in Vietnam. The initial findings indicate a single method of knowledge and skill development is not sufficient to assist users to deal with complex and constant changing security needs. It is necessary to further experiment methods of encouraging formal and peer knowledge sharing that can support individual effort in complying with security policies.

Keywords: knowledge sharing, types of security information, social media, security compliance

1 Introduction

Organizations at the verge of information security risks due to higher data breaches. Although organizations are putting in place technical measures, Juniper Research predicts data breaches would cost $8 trillion globally by 2022 (Juniper Research 2017). However, it is human factor that causes most organisational security risks as security incidents are indirectly caused by employees often failing to comply with organizational polices (Pattabiraman 2018).

Prior studies have established that users' internal factors such as attitude, self-efficacy and perceived response cost towards security tasks can affect their commitment to complying with information security policies (Safa et al. 2016; Sommestad et al. 2015). Security self-efficacy describes an individual's security knowledge and expertise that enables him/her to perform their security tasks, as well as cope with changing security requirements. Contrary to this above, lacking cyber security knowledge could results in users' lack of confidence, higher dissatisfaction, and a sense of helplessness (Salanova et al. 2013), causing confusion to deal with security incidents in practice (Tarafdar et al. 2011). As a result, employees often struggle to find a solution to deal with cyber security issues.

Role of knowledge sharing among employees is paramount for business success. Knowledge sharing in relation to information security is often achieved through training and through provision of security policy procedures (Park 2017; Puhakainen and Siponen 2010). Encouraging knowledge sharing among employees can enhance their understanding of organizational issues and promote their commitment (Park 2017). However, few studies have examined how employees practice knowledge sharing in the context of cyber security (Rocha et al. 2014), and whether to use knowledge acquisition and sharing at work as the potential channels to improve the cyber security system internally. Furthermore, researchers found that these methods often remain inefficient in the dissemination of required knowledge. For example, the complexity and technical aspects of information security knowledge are often seen prime inhibitors at individual level among employees (Safa and Von Solms 2016).

This study aims to explore what types of security information that employees discuss and share on various communication methods at work and assess their impacts on users' security practice. By acquiring better understanding of sharing methods on user security behaviour, organisations can design and develop suitable channels to increase their employees' cyber security knowledge and encourage their security compliant commitments. The next section presents the significance of knowledge sharing in security practice, followed by a review of knowledge sharing channels. Next proposed study method and initial findings are provided. Lastly, future research is outlined.

2 Significance of Security Awareness and Knowledge Sharing to Security Compliance

Of the three types of information security measures (i.e. physical, technical and administrative), effectiveness of administrative measures relies greatly on levels of awareness and compliance among IT users. Administrative security measures are mainly specified in information security policies (Höne and Eloff 2002). In fact, most research on security compliance has focused on understanding factors influencing users to comply with security policies (Safa 2018; Sommestad et al. 2014). Lack of sufficient cyber security awareness can lead to the unsafe behaviour which can pose as a threat to the proactive safeguarding in organisations (Knapp et al. 2006).

Previous research has shown that knowledge sharing among users within an organisation is an efficient way to increase the awareness of employees and their compliance with information security policies (Mallinder and Drabwell 2013; Safa and Von Solms 2016). Given the increasing number of cyber risks, the issue of effective knowledge sharing is more critical to ensure employees stay vigilant against potential risks. Furthermore, complex tasks such as securing information assets cannot be completely accomplished without an efficient knowledge sharing process (Jafari and Charband 2016; Zhang et al. 2012).

Cummings (2004) describes two approaches of knowledge sharing: formal method including disseminating information security policies and formal trainings. Warkentin et al. (2011) found that through informal sharing methods such as support from colleagues, informational material, verbal discussions, feedback sessions and observations help individuals to improve the security behavior and policy compliance. Feledi et al. (2013) emphasized the need of trust among the staff members to enhance the information security knowledge sharing. Safa and Von Solms (2016) discussed the importance of experts and staff with the capabilities of information security knowledge are effective means to enhance security behavior. Several factors have been identified to affect effective security knowledge sharing are

connection between practice and needs of end-users, communication method of security policies and security support services (Jafari and Charband 2016).

Design of information security practices is important since it is an efficient way to generate positive feelings and willingness of employees towards the information assets protection behaviour (Belsis et al. 2005). However, due to emerging threats in the cyberspace often security policy documents become outdated (Liu et al. 2011), leading to higher threats to overall organization (Rocha et al. 2014). In this regard, support from IT experts and peers is important to encourage employees to keep up to date with information protection techniques (Pham et al. 2016; Wang and Hou 2015). By developing a culture where people are always willing to share knowledge and have a trusted and effective channel to communicate, an organisation is not only be able to encourage their employees to improve the knowledge but also to reduce the potential external attacks by increasing the awareness level of information safety and compliance towards the policies internally (Safa 2018).

3 Three Methods of Awareness-Raising in Cyber Security

The first method of raising user security awareness is formal training which has been regarded highly effective in sharing knowledge and developing safe security behaviour of employees (Puhakainen and Siponen 2010). Training has been found as an efficient way to deliver theoretical explanations that are necessary for users to understand 'why' and 'how' of information security compliance (Clark 2008). Training also involves people to think and apply the cognitive thinking about a specific issue or problem they face in information security context (Clark 2008). The cognitive process includes variety of thinking levels in the learning process, including 'remembering, understanding, applying, analysing, evaluating and creating levels (Idris 2016; Meerbaum-Salant et al. 2013). The cognitive process can encourage people to have the critical thinking enabling self-regulation, which directly lead to the stable and long-term sustained behaviours.

The second method is through virtual communities and social media platforms which have emerged as a new way of group knowledge sharing, which allow people to share information and experience without meeting face-to-face (Chang et al. 2015). Social media offers more cooperative platform to share thoughts, experiences, opinions, feedbacks and perspectives (Kaplan and Haenlein 2010). Furthermore, social media platforms offer a better way to acquire new knowledge from peers, networks and through live engagements (Wasko and Faraj 2000). Additionally, information is disseminated through variety of methods including videos, photos and audios (Kwahk and Park 2016). Although, the role of social media as knowledge sharing platform is well recognized (Gupta and Brooks 2013; Hajli and Lin 2016), however, the use of social media for security knowledge sharing within an organisational workplace has been neglected.

The third one can be done through designated information security experts in each department. A departmental security expert refers to an individual who is recognised for being knowledgeable and having more domain technical skills than other colleagues. By facilitating the knowledge sharing within a specific working community, departmental experts can reduce the waiting time and cost for their organisation from investing in cyber security technical system (Safa et al. 2016). There are two types of departmental experts, including formal ones such as managers or supervisors, and informal ones, any single employee who is respected from others toward a security field. Supervisory support was found to be an important factor that increases knowledge sharing among employees by reinforcing positive attitudes and feelings of employees (Shafiq et al. 2013). Such support can be expressed implicitly through the reactions of supervisors when managing mistakes, thus, positively influence the adapting efforts, self-responsibility, collaboration and knowledge sharing of employees towards the expected environments in workplace (Raineri and Paillé 2016). In addition, with the control and discretionary power to make decisions, managers are able to allocate training schedules, develop training strategies, and build competence programs and act as potential channels for providing advices for specific security problems (Kettinger et al. 2015).

On one end, guarding the organisation's IS against cyber-attacks is critical and improving users' awareness and skills is a common approach to any security program. On the other end, organisations lack a clear understanding in determining what types of IS security information should be delivered through various methods of communication to be effective in boosting users' knowledge and compliance behaviour. The study sets out to ascertain how business users perceive the effectiveness of three identified knowledge-sharing methods on their security practice. The expected findings would elaborate how suitable platforms for encouraging knowledge sharing practice among users can improve security awareness and skill development, which may lead to better security compliance.

4 Research Method

This study employs qualitative approach using semi-structured group interviews to explore security knowledge/information sharing practice among employees in organisations. Interview questions were open-ended, enabling researchers to discover, comprehend and get the insights of the participants on how they perceive and assess effectiveness of various knowledge sharing methods (Denzin and Lincoln 2018). The subject of this study concentrates on employees and their interaction with security communication, hence only end business users are to be recruited for the interviews. Managers of several organisations that the researchers had connections with were contacted to join the study. Accepted organisations were asked to recommend available employees to participate the interviews. So far eight interviews, averaging 45 to 60 minutes each, with 25 participants from eight organisations were conducted. Participants were asked to provide years of work experience in the company, job position, department, level of IT expertise and their experience of discussing cyber security issues at work.

Since multiple interviews were conducted, the findings from previous interviews were used guide the following ones to explore more aspects or confirm previous findings of security knowledge sharing practices. By interviewing users from different organisations, the diverse security environments in different organisations enabled to explore a range of security practices. Due to inherent complexity and unclarity of security concepts, participants were shown a set of photos (e.g. security warning icons and logos, physical security artefacts) depicting different security-related factors that might gauge the participants' experience and thoughts towards cyber security. The interviews were conducted in both English and Vietnamese, and the Vietnamese ones were transcribed into English. The answers of participants were transcribed, coded, and grouped by common key themes using Nvivo version 11, a text analysing software for qualitative research. From the transcripts, data were filtered and classified to identify and elaborate participants' responses on information types and sharing methods.

5 Initial Study Results

There are diverse views towards topics to be communicated on each method. Most participants agreed that they did not discuss or share security topics among colleagues, rather they should be directed to IT staff. When employees face some risky situations, they normally prefer to call IT staff for help. Security training is still the main method to provide awareness and skills to comply with security policies. Though this method is far from satisfying users' needs due to lacking timely and up to date guidance. Most participants agreed that alternative methods of peer sharing of security topics can be important and helpful for paying attention to their security practice.

5.1 Security Training for Policy Updates

Training was commonly agreed among participants as a common and effective method to equip employees with necessary security knowledge and come along with the suggestion that it need to be customised with different working natures. Majority of participants agreed that the IT department could provide more training courses and send employees to workshops to update their knowledge about cyber security. Responses from participants also viewed IT training as providing too technical and unfamiliar knowledge in an unattractive format to most users. They insisted that trainings that contain fun, interactive and authentic activities would stimulate more interest.

Many also raised concerns that trainings were not conducted frequently enough and focused more on educating policies than how to deal with security risks. Users may not find them useful in day to day or security crisis.

5.2 Social Media for Instant Major Security Updates

Participants from local financial organisations reported the use of several social media application at work as an unofficial group information sharing channel. Some of these social professional groups comprised more than fifty people from both inside and outside an organization, although the details of these communications were confidential. Groups of stock traders or advisers daily used social media tools such as Facebook Messenger, Skype and Zalo (a local Vietnam developed chat application). Using social media applications for knowledge sharing is preferred by the participants because of its convenience and immediateness without being attached to a computer, which allows employees to share and update their knowledge relating to the information security faster and in a more timely manner.

Most participants preferred using social media to share urgent and significant security warnings to the use of organisational emails. Additionally, information posted on social media should be framed to directly relate to each group's interest to avoid flooding irrelevant updates on their professional

channels. However, many of them were not aware of any security implications using social media. Furthermore, they were not aware of consequences that may occur from disclosing financial information on potentially open and unsecure channels that may end up with people outside the organisation

5.3 Departmental Experts as a Domain-Specific Source for Security Knowledge

Many participants recommended the use of department experts as unofficial security support to new staff members due to their domain knowledge and deep understanding of security culture. Seeking their advice was viewed as an effective way of resolving immediate security tasks without going through time-consuming IT support channel.

Participants highlighted that some organisations did not have formal staff orientation for new staff, who normally did not have sufficient domain knowledge to properly respond to security issues at the right time and right place, which other formal channels could not prove effective. Therefore these experts can provide them with task-related security knowledge and requirements. Sharing knowledge between a designated security expert to other colleagues is, therefore, not only another potential way to enhance knowledge of employees about information security but can also be a cost-effective approach in solving security compliance problems.

6 Future Research

The study's initial findings indicate that initiating regular informal information and knowledge sharing among employees can be effective in improving users' situational awareness and security compliance. Employees tend to take cautions right after a major security incident and soon losing attention afterwards. Initial findings show that organisations still rely on formal training courses to equip users with required awareness. Whereas employees criticise that training does not provide timely and updated knowledge at the time of dealing with security incidents. Given the popularity and anywhere, anytime of mobile technology, organisation can explore use mobile social media tools to facilitate and encourage employees in sharing timely and contextual security knowledge and concerns. Though precautions need to be taken when sensitive security information is shared on these tools. Departmental experts have been found to be valued among participants thanks to quick access to advice for unique business requirements.

It is important for organisations to develop the robust knowledge sharing practice with supporting channels that utilise latest technology development in social media and mobile technology. Next stage of the study will focus on expanding specific types of information advice and contextual use of that information on which sharing methods and how they affect employees' security practice. More emphasis will also be put on detailing how a comprehensive security communication strategy can be developed to cover most aspects of users' security information needs.

7 References

Belsis, P., Kokolakis, S., and Kiountouzis, E. 2005. "Information Systems Security from a Knowledge Management Perspective," *Information Management & Computer Security* (13:3), pp. 189-202.

Chang, C. M., Hsu, M. H., and Lee, Y. J. 2015. "Factors Influencing Knowledge-Sharing Behavior in Virtual Communities: A Longitudinal Investigation," *Information Systems Management* (32:4), pp. 331-340.

Clark, R. C. 2008. *Building Expertise: Cognitive Methods for Training and Performance Improvement*. John Wiley & Sons.

Cummings, J. N. 2004. "Work Groups, Structural Diversity, and Knowledge Sharing in a Global Organization," *Management Science* (50:3), pp. 352-364.

Denzin, N. K., and Lincoln, Y. S. 2018. *The Sage Handbook of Qualitative Research*, (Fifth edition. ed.). Los Angeles: Sage.

Feledi, D., Fenz, S., and Lechner, L. 2013. "Toward Web-Based Information Security Knowledge Sharing," *Information security technical report* (17:4), pp. 199-209.

Gupta, R., and Brooks, H. 2013. *Using Social Media for Global Security*. John Wiley & Sons.

Hajli, N., and Lin, X. 2016. "Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information," *Journal of Business Ethics* (133:1), pp. 111-123.

Höne, K., and Eloff, J. H. P. 2002. "Information Security Policy — What Do International Information Security Standards Say?," *Computers & Security* (21:5), pp. 402-409.

Idris, G. 2016. "The Evaluation of the Cognitive Learning Process of the Renewed Bloom Taxonomy Using a Web Based Expert System," *TOJET : The Turkish Online Journal of Educational Technology* (15:4).

Jafari, N. N., and Charband, Y. 2016. "Knowledge Sharing Mechanisms and Techniques in Project Teams: Literature Review, Classification, and Current Trends," *Computers in Human Behavior* (62), pp. 730-742.

Juniper Research. 2017. "Cybercrime & the Internet of Threats." Retrieved 30 May, 2018, from https://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats-2017

Kaplan, A. M., and Haenlein, M. 2010. "Users of the World, Unite! The Challenges and Opportunities of Social Media," *Business Horizons* (53:1), pp. 59-68.

Kettinger, W. J., Li, Y., Davis, J. M., and Kettinger, L. 2015. "The Roles of Psychological Climate, Information Management Capabilities, and It Support on Knowledge-Sharing: An Moa Perspective," *European Journal of Information Systems* (24:1), pp. 59-75.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., and Nelson Ford, F. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security* (14:1), pp. 24-36.

Kwahk, K.-Y., and Park, D.-H. 2016. "The Effects of Network Sharing on Knowledge-Sharing Activities and Job Performance in Enterprise Social Media Environments," *Computers in Human Behavior* (55), pp. 826-839.

Liu, D., Ji, Y., and Mookerjee, V. 2011. "Knowledge Sharing and Investment Decisions in Information Security," *Decision Support Systems* (52:1), pp. 95-107.

Mallinder, J., and Drabwell, P. 2013. "Cyber Security: A Critical Examination of Information Sharing Versus Data Sensitivity Issues for Organisations at Risk of Cyber Attack," *Journal of Business Continuity & Emergency Planning* (7:2), p. 103.

Meerbaum-Salant, O., Armoni, M., and Ben-Ari, M. 2013. "Learning Computer Science Concepts with Scratch," *Computer Science Education* (23:3), pp. 239-264.

Park, S.-K., Lee, S.-H., Kim, T.-Y., Jun, H.-J., & Kim, T.-S. 2017. "A Performance Evaluation of Information Security Training in Public Sector," *Journal of Computer Virology and Hacking Techniques* (13:4), pp. 289-296.

Pattabiraman, A., Srinivasan, S., Swaminathan, K., & Gupta, M. 2018. "Fortifying Corporate Human Wall: A Literature Review of Security Awareness and Training," in *Information Technology Risk Management and Compliance in Modern Organizations,* R.S. M. Gupta, J. Walp, & P. Mulgund (Eds.) (ed.). Hershey, PA: IGI Global, pp. 142-175.

Pham, C. H., El-den, J., and Richardson, J. 2016. "Stress-Based Security Compliance Model-an Exploratory Study," *Journal of Information and Computer Security* (24:3), pp. 326-347.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757–778.

Raineri, N., and Paillé, P. 2016. "Linking Corporate Policy and Supervisory Support with Environmental Citizenship Behaviors: The Role of Employee Environmental Beliefs and Commitment," *Journal of Business Ethics* (137:1), pp. 129-148.

Rocha, F. W., Antonsen, E., and Ekstedt, M. 2014. "Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture," *Computers and Security* (43), pp. 90-110.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. 2018. "Motivation and Opportunity Based Model to Reduce Information Security Insider Threats in Organisations," *Journal of Information Security and Applications* (40), pp. 247-257.

Safa, N. S., and Von Solms, R. 2016. "An Information Security Knowledge Sharing Model in Organizations," *Computers in Human Behavior* (57), pp. 442-451.

Safa, N. S., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56), pp. 70-82.

Salanova, M., Llorens, S., and Cifre, E. 2013. "The Dark Side of Technologies: Technostress among Users of Information and Communication Technologies," *International Journal of Psychology* (48:3), pp. 422-436.

Shafiq, M., Zia-ur-Rehman, D. M., and Rashid, M. 2013. "Impact of Compensation, Training and Development and Supervisory Support on Organizational Commitment," *Compensation & Benefits Review* (45:5), pp. 278-285.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 42–75.

Sommestad, T., Karlzén, H., and Hallberg, J. 2015. "The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance," *Information and Computer Security* (23:2), pp. 200-217.

Tarafdar, M., Tu, Q., Ragu-Nathan, T., and Ragu-Nathan, B. 2011. "Crossing to the Dark Side: Examining Creators, Outcomes, and Inhibitors of Technostress," *Communications of the ACM* (54:9), pp. 113-120.

Wang, W.-T., and Hou, Y.-P. 2015. "Motivations of Employees' Knowledge Sharing Behaviors: A Self-Determination Perspective," *Information and Organization* (25:1), pp. 1-26.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems* (20:3), pp. 267-284.

Wasko, M. M., and Faraj, S. 2000. "“It Is What One Does”: Why People Participate and Help Others in Electronic Communities of Practice," *The Journal of Strategic Information Systems* (9:2), pp. 155-173.

Zhang, X., Pablos, P. O. d., and Zhou, Z. 2012. "Effect of Knowledge Sharing Visibility on Incentive-Based Relationship in Electronic Knowledge Management Systems: An Empirical Investigation," *Computers in Human Behavior* (29:2), pp. 307-313.