An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice

Hiep Cong Pham
RMIT University Vietnam
Viet Nam
hiep.pham@rmit.edu.vn

Irfan Ulhaq
RMIT University Vietnam
Viet Nam

Minh Nhat Nguyen
RMIT University Vietnam
Viet Nam

Mathews Nkhoma
RMIT University Vietnam
Viet Nam

Abstract

In a networked global economy, cyber security threats have accelerated at an enormous rate. The security infrastructure at organisational and national levels are often ineffective against these threats. As a result, academics have focused their research on information security risks and technical perspectives to enhance human-related security measures. To further extend this trend of research, this study examines the effects of three knowledge sharing methods on user security practices: security training, social media communication, and local security experts (non-IT staff). The study adopts a phenomenological method employing in-depth focus group interviews with 30 participants from eight organisations located in Ho Chi Minh city, Vietnam. The study expands on understanding factors contributing to self-efficacy and security practice through various knowledge sharing channels. Current methods of periodical training and broadcast emails were found to be less effective in encouraging participants to develop security self-efficacy and were often ignored. Security knowledge sharing through social media and local experts were identified as supplementary methods in maintaining employees' security awareness. In particular, social media is suggested as a preferred channel for disseminating urgent security alerts and seeking peer advice. Local security experts are praised for providing timely and contextualised security advice where member trust is needed. This study suggests that provisions of contemporary channels for security information and knowledge sharing between organisations and employees can gain regular attention from employees, hence leading to more effective security practices.

Keywords: knowledge sharing, social media, cyber security, security compliance

1 Introduction

The security risks to an organisation's sensitive information are constantly growing. Both external and internal attacks are becoming more sophisticated and persistent (Sindiren & Ciylan, 2018). Juniper Research (2017) predicts data breaches will cost $8 trillion globally by 2022. Technical measures have been effective and robust in preventing cyber risks from

information security breaches (Rocha et al., 2014). However, research also shows that a majority of organisational security incidents are directly or indirectly caused by employees who violate or neglect the information policies of their organisations (Ashenden, 2008; Sindiren & Ciylan, 2018). Employee compliance choices are therefore critical to organisational security (Sommestad et al., 2014), and overcoming this challenge requires more than technical measures.

Prior studies have established that users' personal factors such as attitude, self-efficacy, and perceived response costs associated with security tasks can affect their intention to comply with information security policies and practices (Sommestad et al., 2015). Additionally, knowledge about cyber security and motivation to protect from cyber risks are necessary to enhance cyber security practice. Security self-efficacy, which is the combination of an individual's security knowledge, skills, and expertise, enables the individual to perform security tasks and cope with changing security requirements. A lack of knowledge about information security leads to low levels of employee engagement in cyber security practice, jeopardising the organisation's information security (Pham et al., 2016).

Knowledge about cyber security is often achieved through training (Puhakainen & Siponen, 2010). Training often consists of formal dissemination of security information (e.g. policies), as well as procedural, technical knowledge (Park et al., 2017). Current training methods are often seen as inefficient at disseminating security knowledge to non-technical employees, mainly because of the complexity and technical aspects of information security knowledge (Safa and Von Solms, 2016). Lengthy policies and training materials often lack simplicity for an average user and technical information in policy documents remains complex (Pham et al, 2019).

Another way of developing security knowledge can be facilitated through collaborative sharing among employees (Hwang & Kim, 2007; Wang & Noe, 2010). The effectiveness of collaborative networks for knowledge sharing is evident in other areas such as medicine (Oh, 2012) and hospitality (Yang, 2009). Building an employee culture of proactively raising awareness and sharing knowledge of information security matters has recently been debated across disciplines (Schlienger & Teufel, 2002). Since humans are key assets of every organisation, and most security concerns are human-based, a knowledge-sharing culture helps organisations build trustworthy partnerships among internal communities (Schlienger & Teufel, 2002). However, insecure or inappropriate sharing of information assets could also lead to the potential loss of data or information or could put people into vulnerable situations. In such scenarios where individuals are facing a problematic situation, trustworthy advice and clear guidelines for knowledge sharing becomes significant (Tamjidyamcholo et al., 2013).

Although proper security practice can be learned through formalised procedures, there are certain tasks which require more practical instructions and timely advice of information security. An employee might unintentionally violate the security policy of an organisation, which could place them and the organisation at risk. To address this, researchers place a high stake on workplace knowledge sharing through social exchanges and informal peer discussions. Safa & Von Solms (2016) discuss the potential benefits of an information sharing culture and how it can improve staff efficacy regarding security awareness, promote sharing knowledge on policies and procedures, and lead to compliance improvements in security programs. However, few research studies have examined how employees practice knowledge sharing in the context of cyber security (Rocha et al., 2014). Furthermore, it is not known whether and how such practices affect security behaviour in the workplace.

Consequently, this study explores how employees acquire and share security information at work and assesses the impacts of such knowledge sharing practices on employees' security self-efficacy and practice. The study employed a qualitative phenomenological method of in-depth focus group interviews with employees in various organisations located in Ho Chi Minh city, Vietnam. The findings contribute to both theoretical and practical aspects of employing various security knowledge sharing methods to influence employees' efforts to maintain security awareness and practice.

2 Significance of knowledge sharing to security awareness and practice

Organisations manage information security through a combination of administrative and technical measures. Administrative measures aim to encourage safe security practices and deter malicious computer abuses through security policies and procedures, awareness training, and security compliance supervision (Crossler et al., 2013). However, the effectiveness of administrative measures relies greatly on the levels of awareness and compliance among IT system users. Technical measures ensure safe security practice through the use of authentication, authorisation, data encryption, and antivirus software, as well as a myriad of hard and soft system elements designed to prevent breaches and encourage desired behaviours (Powell, 2018). Previous research has shown that knowledge sharing among users within organisations is an effective way to increase awareness of and compliance with information security policies (Mallinder & Drabwell, 2013; Safa & Von Solms, 2016). Given the increasing number of cyber risks, effective real-time knowledge sharing could help employees protect the organisation against potential security risks (Torres & Gupta, 2018).

To decrease cyber risks from users, the risks need to be apparent to users and they need to understand their role in decreasing these risks. If users are not aware of cyber security issues, and if they do not have sufficient self-efficacy to respond, security threats cannot be addressed (Safa et al., 2016). In addition to awareness of security risks, knowledge about appropriate responses is necessary if cyber risks are to be reduced. Awareness of the risk is necessary, but is insufficient at reducing risk alone; people must also know how to act in situations of security breaches (Popovac & Fine, 2018). Security risk awareness and skills are generally referred as self-efficacy, which encompasses "a belief in one's capability to protect information and information systems from unauthorised disclosure, modification, loss, destruction, and lack of availability" (Rhee et al., 2009). High levels of self-efficacy mean knowledgeable and skilful employees are more likely to take protective security tasks. A lack of self-efficacy has also been found to be a major contributor to cyber security compliance disengagement (Pham et al., 2016; Pham et al., 2019).

Recent literature on knowledge sharing advocates a socio-technical perspective and posits that knowledge does not only reside in documents and systems but also in people's minds (Brown & Duguid, 1999; Nonaka & Takeuchi, 1995). Furthermore, knowledge sharing is a joint approach between sender and receiver, resulting in individual learning, and positively impacts organisational learning (Ipe, 2003). It is important for organisations to understand that tacit knowledge (or 'know-how') is a sticky concept, hard to share completely, and is not always easy for a receiver to understand at full scale (Nonaka et al., 2006).

Another factor that influences cyber security compliance is that of task complexity. Complex tasks required to secure information assets cannot always be accomplished without an

effective knowledge sharing process (Jafari & Charband, 2016; Zhang et al., 2012). Complexity becomes an issue in cyber security when the risk is difficult to comprehend by a lay-user (Zhang & Costa, 2018). In such cases, peer networks and social learning are useful in decreasing the overall fear of engagement that often pervades a high-risk IT environment (Warkentin et al., 2011). By applying a social learning theoretical lens to the healthcare sector, Warkentin et al. (2011) found that informal sharing methods such as support from colleagues, sharing materials, informal verbal discussions, feedback sessions, and observations helped individuals to improve their security behaviours and compliance with policy.

3 The effect of three knowledge sharing methods on security practice

Knowledge sharing enables employees to develop ideas, share information about security concerns, and collaborate within the workplace environment about cyber information threats (Rocha et al., 2014). Cummings (2004) describes two approaches to knowledge sharing: formal methods, including disseminating information security policies and formal training (Höne & Eloff, 2002), and informal methods, comprising of conversations, peer to peer discussions, and advice-seeking and sharing.

Given the starting point of multiple methods of knowledge sharing, this study focuses on assessing the effects of three forms of knowledge sharing: formal training programs, social media communication, and local security experts on employees' security awareness and practice.

3.1 Formal security training

Training programs are a popular form of disseminating knowledge and developing safe information security behaviour in employees (Puhakainen & Siponen, 2010). Training is an efficient way to deliver the theoretical explanations that are necessary for users to understand why and how security compliance can help users protect the information assets of an organisation (Clark, 2008). Training can also improve self-efficacy and self-regulation of information security behaviour (Clark, 2008). However, security training can also change attitudes and behaviours towards a specific issue without users actively thinking or deeply analysing and considering the issue (Puhakainen & Siponen, 2010). Furthermore, training builds on prior understandings and abilities, and ensuring learners' security knowledge levels are at a commensurate level can be challenging (Park et al., 2017). Consequently, training on its own is insufficient to completely ameliorate cyber security risks, and other forms of knowledge sharing are necessary.

Training offers not only a better chance to directly transfer knowledge to the employees, but it also allows the organisations to develop the content with the strong relation to the organisation's policies (Brandl, 2012). Knowledge sharing through training and close collaboration can build trust among employees and can further develop a secure environment (Liu et al., 2011; Safa & Von Solms, 2016). Trust is an important mechanism in enhancing knowledge sharing between employees and is therefore a necessary precursor to securing the cyber environment (Feledi et al., 2013).

The effectiveness of programs on changing cyber security practices depends on how the information has been shared with users. Khan et al (2011) noted that face-to-face training is more effective than computer-based training. This is because users' cyber security actions can

be built on understanding the consequences of a compromised security system (Rhee et al., 2009) and the reasons for developing security policies and procedures (Pham et al., 2019), thus face-to-face training can raise cyber security awareness of employees. Furthermore, face-to-face education is also more economically viable than computer-based training, which usually requires more physical and technical resources.

Computer-based training, however, has the advantage of one-on-one communication. It allows users to practice at their own pace, which prevents users from becoming overwhelmed by information (Khan et al, 2011). Since the nature of computer-based training is ready-made, it often lacks direct interactions between organisations and employees, and is difficult to reflect the organisation's policies (Brandl, 2012; Khan et al, 2011).

3.2 Social media communication of security updates

With the dramatic development of communication technologies, virtual communities on social media platforms have emerged as a new way to share knowledge. These communities allow people to share information and experience without meeting face-to-face (Chang et al., 2015). Furthermore, these communities are available when and where the user needs them, via any device and in a format they can access given their skills and capabilities. Rather than providing information passively, social media offers more cooperative and open communication, where a large number of people are free to share any of their thoughts, experiences, opinions, feedback, and perspectives (Kaplan & Haenlein, 2010). The increased mobility of social media and the popularity of smartphones has made social media use a daily activity (Kwahk & Park, 2016). Social media platforms offer an effective way to acquire new knowledge from peers and networks (Wasko & Faraj, 2000). Social media tools therefore operate as a knowledge management system, as they permit a flexible mode of dialogue and sharing information in several formats (Kwahk & Park, 2016; Oostervink et al., 2016). Each of these capabilities enables real-time problem solving by IT professionals and others within the community, potentially minimising any damage from cyber threats.

In addition to flexible social structures and immediacy, social media enables the dissemination of knowledge and information in multiple forms such as videos, photos, audio, comments, or blog posts. This permits community members to share knowledge in whatever form is most natural for them at the time (Kwahk & Park, 2016).

The role of social media as a knowledge-sharing platform is well recognised, but research on the use of social media in communicating cyber security information is scarce (Aloul, 2012; Gupta and Brooks, 2013; Hajli & Lin, 2016). This is potentially due to the security risks associated with social media in general (e.g. Pattabiraman et al., 2018; Zhang & Costa, 2018). However, there has been research in a university setting that has shown that social media can be effective in a knowledge sharing context (Aloul, 2012). Hence, it is timely to evaluate the influence of knowledge sharing through social media on cyber security practice.

3.3 Local security experts (non-IT professional staff) providing domain-specific knowledge

When it comes to delivering cyber security knowledge, time and place of the support is critical. Having at least one information security expert or 'champion' in each department has been shown to be effective (Ashenden, 2008; Cherdantseva et al., 2016). A local security expert is responsible for answering security concerns of others, identifying potential threats, and reminding others to comply with security policies. In order to carry out such responsibilities,

the local expert is normally recognised as having more experience and skills than the 'average' user. By facilitating knowledge sharing within a specific work community, local experts can also reduce waiting times and costs associated with computer down-time (Safa et al., 2016) by being immediately available to assist. These 'champions' may not be formally appointed but may be evidenced merely by their contributions to their departments. There are two types of local experts: formal, such as managers, and informal, such as any individual employee who is respected by others when it comes to cyber security.

Manager's support has been found to be an important factor in facilitating knowledge sharing. It increases knowledge sharing among employees by reinforcing positive attitudes of employees towards cyber security measures (Shafiq et al., 2013). Such support can be expressed implicitly through the reactions of supervisors when managing mistakes, consistent and equal treatment of employees, competences of supervisors that relate to technical aspects, and the supervisors' willingness to support and protect employees in front of other managers (Shafiq et al., 2013). Managerial support can therefore positively influence the efforts required to adapt to change, user-responsibility towards security issues, levels of collaboration with others, and knowledge sharing (Raineri & Paillé, 2016). Furthermore, employees' belief in their managers' knowledge and expertise was found to positively affect employees' self-reported security breaches (Liao, 2008; Mittal & Dhar, 2015), demonstrating employees' willingness to co-create a secure environment. With the control and discretionary power to make decisions, line managers are able to allocate training schedules, develop training strategies, build competence programs to increase the relevant knowledge of their employees, provide valuable feedback, create an open working environment, enhance engagement levels, and promote information sharing among employees (Kettinger et al., 2015; Ramus & Steger, 2000). Finally, with high information security knowledge and skills, local security experts can be a potential channel for advice on specific security problems and facilitating security knowledge exchange among employees.

In summary, many previous studies support the important role of user self-efficacy in achieving safe security practice and efforts to employ security technologies (Bulgurcu et al., 2010; Johnston and Warkentin, 2010; Rhee et al., 2009). Improving users' self-efficacy through knowledge and practice sharing is a common approach to any security program to achieve more effective security practice. However, organisations often lack a clear understanding of how various knowledge sharing practices can influence users' effort to acquire security skills and their resulting practice. This study therefore sets out to ascertain how employees perceive the effectiveness of the three identified knowledge-sharing methods on enhancing their self-efficacy which subsequently improves security practice.

The arguments put forward in this study is summarised in Figure 1.

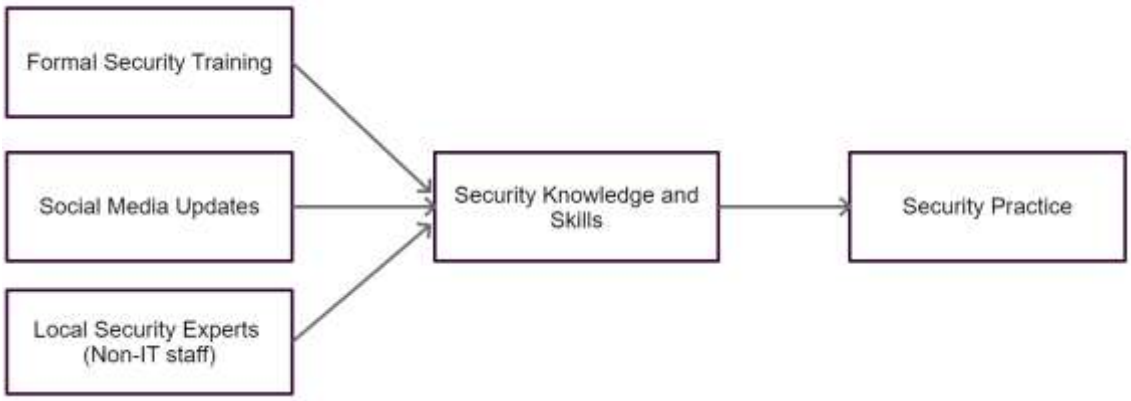

Figure 1: Conceptual model of cyber security knowledge sharing

4 Study methodology

We focus on developing a deeper understanding of several individuals' common experiences of acquiring security information through various methods and how such knowledge impacts their and their own daily practice at work. Such insights help develop more focused training programs and policies. Exploring lived experiences of a phenomenon such as security practice to gain in-depth understanding of underlying reasons contributing to such practice requires a phenomenological method (Cilesiz, 2011; Creswell, 2007). The purpose of a phenomenological study is to establish essential elements of common experiences among participants (Moustakas, 1994). It is important to note that a phenomenological approach acknowledges the key common experience can change and be incomplete (Moustakas, 1994). The results of this study therefore do not claim to represent a universal truth, but rather the shared security practices at a specific time and place, as manifest in the participants' experiences and as seen from the perspective of an individual researcher.

Another requirement of phenomenological research is that there are no prior assumptions about the correctness or falsity of a participant's experience of the phenomenon (Ashworth, 1999). Hence before starting the interviews, we did not start with a set of well-formed hypotheses, but instead looked for common practices that emerged through a series of interviews and used other participants to validate our findings. The participants were encouraged to freely share their own perspectives to provide insight into their security experiences.

Criterion sampling was employed so that only participants who share or receive relevant security information at work would participate in the study. This sampling technique is recommended for phenomenological study in Creswell (2007). For data collection, in-depth interviewing was used to ask the participants how they managed their day-to-day lives and personal experiences in relation to cyber security. In depth interviewing is well suited to collecting personal experience descriptions (Creswell, 2007).

We approached 12 organisations with whom we had worked in the past for suitable employees to interview. Eight organisations agreed to join the study. Participants were selected from a range of departments, who could provide diverse perspectives of their security practices. Thirty participants participated in eight in-depth focus group interviews, ranging from 60 to 90 minutes (see Table 1). The number of interviews was considered sufficient when the participants' responses provided a clear picture of the three knowledge sharing practices and

their effectiveness on security practice. As little significant new insights were acquired in the last few interviews, the number of interviews was considered to meet the theoretical saturation criterion for qualitative research established by Dworkin (2012), which indicates the point where no new information or themes are observed in the data.

Organisation	Number of participants	Position and pseudonyms
1. Software retailer	3	Software designer (3.1, 3.2, 3.3)
2. Financial organisation 1	4	Auditors (4.1, 4.2, 4.3, 4.4)
3. Financial organisation 2	4	Financial specialist (3.1, 3.2, 3.3)
4. Financial organisation 3	1	Marketing staff (4.1)
	1	Compliance officer (4.2)
	4	Financial specialist (4.3, 4.4, 4.5, 4.6)
5. Financial organisation 4	3	Financial specialist (5.1, 5.2, 5.3)
	1	Market researcher (5.4)
6. Agriculture exporting organisation	1	Investor relation associate (6.1)
7. University	2	Lecturer (7.1, 7.2)
	2	Professional staff (7.3, 7.4)
8. Marketing organisation	2	Advertising designer (8.1, 8.2)
	2	Marketing staff (8.3, 8.4)

Table 1: Profiles of participants

Participants' responses were analysed following the three-step phenomenal analysis outlined in Moustakas (1994) – phenomenological reduction, imaginative variation, and synthesis – with the help of text analysis software NVivo 11. In the first step, all interviews were conducted face-to-face in both English and Vietnamese (dependent upon the language capabilities of the participants), recorded, transcribed, and translated into English. Researchers then went through the transcripts several times, treating all relevant statements as having equal value. The pre-identified themes of information sharing methods and potential impacts on security practice were used to classify coded responses to enable the researchers to discover, comprehend, and gain insights of the participants. This step was designed to group the responses, eliminate repetitions and overlaps, and produce a list of meaning units (words/phrases that represent only one meaning) across participants. Individual participants' descriptions of their experience of security practice were recorded as quotes together with the researchers' supplementary statements, creating individual textual descriptions. Next, individual structural descriptions or the underlying reasons of participants' day-to-day security experiences were established and transforming participants' statements into security terminology. The final step of phenomenological analysis consisted of synthesising individual textual and structural descriptions of security practice among participants, and constructing textual-structural synthesis. This composite synthesis comes in the form of a final narrative detailing an in-depth description of security practice of the whole group.

The interviews consisted of two parts. The first part asked participants about their security knowledge sharing practices. This part explored how employees discuss and share information related to cyber security within their work environment and their preferred way to share this information. The second part assessed how participants view the effectiveness of

specific knowledge sharing practices on their own security practices. The interview questions are included in Appendix A.

5 Results

5.1 Overview of the roles of security self-efficacy and peer knowledge sharing in security practice

When participants were asked to describe their views of the impacts of knowledge sharing on their security practice, there were mixed responses regarding the necessity of security self-efficacy if security tasks are simple or less obvious to them. Participants from the university highlighted the insignificant role of security skills in their jobs due to task simplicity or unclear expectations:

> *The IT department does all security tasks and they do not require anything from me. So, I am not clear that I must be responsible for the security tasks.* (Lecturer 7.1)

> *I do not think security training is required. Because all security tasks here are quite simple and rare. If users spot a problem, they can report directly to IT department. It does not resemble a scenario that can come up in the training. I have not experienced any security incident that needs a training.* (Professional staff 7.4)

Other participants thought that security tasks are purely for IT professionals or too complex for normal users to assess the risks and take proper care, hence they did not consider it necessary to put effort in maintaining security knowledge and practice:

> *We do not normally update security knowledge, it is necessary to IT professionals. We hardly do that because it is not one of our concerns.* (Financial specialist 4.4)

To some participants, the purposes of enhancing security skills and exercising safe practice are not clear, which means they view it as a waste of time:

> *I see that security compliance is only that you have to comply with organisation's requirements. But I do not see the problem, much on my side why I need to do that. It is much bureaucratic you have to do this, to do that. For the users, I find it too much a waste of time.* (Lecturer 7.1)

Many participants, however, acknowledged they can contribute towards security and that self-efficacy is critical and needs to be learned:

> *Matching computer skills will make me willing to comply. Security tasks could be personalised based on different requirements from different positions in the company. That will support your work better.* (Market researcher 5.4)

Other participants also suggested that to encourage effective security information sharing, organisations could develop a collaborative and open communication culture within teams, fostering the free flow of knowledge, including security knowledge, amongst employees:

> *Culture of the organisation is important. If people are friendly, the information about the risks will be shared quickly to other staff members in the team.* (Financial specialist 3.1)

Most participants agreed they normally did not view sharing security information with their colleagues as an effective way to maintain security awareness or skill building. They did, however, share such information with IT professionals. Sharing security topics was deemed unnecessary in everyday experiences at work. There emerged several reasons for this assessment. Firstly, the rarity of security issues and the relatively low impact of cyber security

on daily work activities meant that it was simply not a topic of conversation. Secondly, even when there was talk about IT security, the information was complex and difficult to understand without technical expertise. Thirdly, participants were not convinced that IT security was urgent enough to resolve the issue through peer-support or independently; they felt that notifying IT department about the issue would be 'enough'. Fourthly, IT security breaches often encompass confidential information and participants felt that IT professionals are better placed to protect information assets than their colleagues. Finally, even if an employee could solve the security issues, since they have different roles and are not dedicated to supporting IT issues, asking for help was seen as a disruption to others.

5.2 Formal training for security awareness

Many participants agreed that training by security professionals is a common method of providing security knowledge and skill enhancement. Security training can equip users with basic knowledge of organisational policies and relevant risks. One participant emphasised the relevance and authenticity of the security cases used in the training that urged them to take security matters more seriously. This view is consistent with findings of Rhee et al (2009), which indicates that security breach experience can affect perceived self-efficacy and how users exert effort in their security practice. One participant confirmed this:

> *Security training needs to show how users' security compliance is important to protect the business. Also, we need mock up exercises through which we can easily understand the severity of the risks and effectiveness of the recommended actions. Then we will follow and support security guidelines actively*. (Marketing staff 8.4)

In addition to security training, the efficacy of IT professionals is important to ensure participants take security advice. A few participants explained that it demonstrates the organisation can be effective to protect information systems:

> *I will take IT staff advice if they show competency, capable of managing the IT security risks, and they give us some knowledge if we follow them. They have to prove that they can do something with the risks for my computer first. From that I will take their advice into account, it should come from a qualified IT department.* (Marketing specialist 8.2)

It was a consensus among participants that training contents need to be customised for different work contexts due to the specific nature of the risks:

> *People might think that cyber security is something that is not related to their job and do not understand about it. Therefore, I think it is necessary to get every employee to engage with the training program. Furthermore, the training should be designed to relate to the jobs' natures to be more relevant and interesting*. (Software designer 1.2).

Participants suggested that formal training programs should be offered periodically to reinforce security knowledge and practice, and that the content formats of such trainings should be more diverse, which many organisations may not consider:

> *We do not have much security training at work. I think security was mentioned briefly during the induction for new staff. After that, there is no further training or updates on what security requirements and skills that staff need to know*. (Financial specialist 3.2).

Participants who had attended security trainings before often suggested more engaging and interactive formats, not simply a reinforcing of instructions. Traditional didactic training

methods were seen as providing too much technical and plain policy information in an unattractive format:

> *Everything about rules and regulations needs to be educated in a creative, smart, and attractive way. Training should provide new knowledge, excite people so that compliance becomes voluntary, not something that rigid, compulsory so 'you have to do it' way*. (Financial specialist 4.6)

Sharing the same view of creating more interesting and engaging training programs, a few participants wanted training that was fun to undertake, including interactive game-like activities that would stimulate more interest and facilitate easy security skills acquisition:

> *I think training programs incorporating game-format competitions will attract more engagement from employees. Game-format interactions make the learning more fun and realistic rather than having to read the policies that company provide*. (Auditor 2.3)

This request is consistent with research into negative emotions and behaviour change, whereby behaviours are more sustained over time if they are associated with positive emotions (Brennan & Binney, 2010).

5.3 Social media for sharing of information security

Participants from financial organisations 2, 3, 4, and 5 reported the use of several social media applications at work as an unofficial information sharing channel. Groups of stock traders or advisers from these organisations used social media tools such as Facebook Messenger, Skype, and Zalo (a Vietnamese chat application) to share market-related information. They used these tools because they are popular, provide instant knowledge sharing, and support multimedia content, including visual and audio files. Some of these social professional groups comprised more than fifty people from both inside and outside an organisation, although the details of these communications were kept confidential from the researchers. When asked to comment on how it would be useful for the organisation to communicate security topics through social media channels, especially in urgent situations, two participants liked the idea:

> *Sending security warnings through Skype is very useful in my company because all staff can join and discuss about the problems easily. If the risk is very important and serious, the organisation can send the information through emails and everybody can spread the news further on Skype.* (Finance specialist 3.3)

> *Most people in my company use and check notifications on the Zalo, therefore, it is easier to get people's attention by using this social media application rather than through formal email channel, which I normally skip reading. If the messages are sent to my Zalo account, maybe I will look at it because it is much shorter, more visual and easier to remember*. (Auditor 2.1)

Using social media applications for knowledge sharing was preferred by these participants because of its convenience, timeliness, and because it can influence their security practice. For example, when someone shared a personal experience of a security incident, such as losing information due to a hard disk crash, losing a social account due to poor password usage, or not carefully checking spoof websites, members in the social group took the advice very quickly and personally. Participants reported formal training that employed traditional methods and hypothetical scenarios did not help them to fully appreciate the serious consequences of poor security behaviour:

> *When I heard someone in my work group lost their Facebook account or all data on the organisation's provided computer due to a hard disk malfunction, I immediately changed my password or asked IT staff how to back up my data.* (Marketing staff 8.3)

Furthermore, participants raised the point that messages shared on social media should be brief (due to the small screens of mobile devices) and visual engaging, to depict the contents more clearly, and to avoid 'TL;DR syndrome' (too long; didn't read). Additionally, social media information needs to be framed to directly relate to each group's interests, to avoid flooding their professional social media with irrelevant updates. Too much irrelevant information can lead to messaging being ignored or avoided:

> *We do not want to receive too many security notices on our social channels. Only very significant and urgent notifications should be sent to these channels. Otherwise we will block or ignore future messages from the IT department*. (Financial specialist 3.3)

A few participants suggested that email communications were not as effective as social media as a means of sharing knowledge and improving awareness. This was because the email content was considered plainer and more tedious to read than the visually rich content of social media platforms.

While most participants preferred using social media to share important security information to organisational emails, many of them were not aware of the security risks of using social media. They were also not aware of the consequences of disclosing financial information on potentially open and unsecure channels, which may include people outside the organisation. However, if people are using social media anyway to make their information lives easier, organisations may be able to take this into consideration when designing cyber security knowledge sharing systems.

5.4 Local security experts (non-IT professional staff) for sharing context-specific security knowledge

Many participants suggested that new employees often lacked adequate knowledge when dealing with minor security issues, particularly when they were unfamiliar with the issues or the organisation's requirements. Other sources of security information such as training may not be readily available at the time of need and formal policies do not cover all jobs' security risks. Some participants shared that their local security experts, who could be senior staff or simply someone who has more experience of the security context, can be a valuable resource for assisting staff with security protection. For example, one participant explained:

> *At previous workplaces, I did not have any training course on cyber security. However, from starting at this organisation, my senior was the one who trained and gave me advice about the information protection.* (University staff 7.4)

Most participants agreed that a local security expert can be an alternative for employees seeking security advice or solutions, rather than relying solely on the IT department. Moreover, because a local security expert is perceived as part of the employees' peer group, they can often provide better and more relevant advice to their colleagues (e.g. based on their experience of the job requirements) than IT staff. Trust and respect between employees and the local experts were also identified as important. A high level of trust among colleagues and local security experts could initiate open discussions on security issues, in both non-critical and critical incidents.

Some participants mentioned that they had taken immediate actions to change passwords and perform backup of their laptops when they heard of security breaches experienced by colleagues, as it was both relevant to their day-to-day activities and genuine enough that it required urgent action. A participant explained:

> *During a lunch, my colleague told her laptop got a hard disk crash and all data was lost. IT staff was trying to recover it. I was shocked to think it could happen to me a s well. So, I contact IT department to assist with data protection immediately*. (Professional staff 7.3)

Others agreed that peer sharing of security topics is important and helpful for their security practice. Peer sharing is also both authentic and relevant to solving cyber security problems among employees. For example, one participant stated:

> *Information shared from other colleagues is important because it directly relates to my job. Furthermore, staff information sharing such as during lunch will help me to understand more about the problems*. (Auditor 2.4)

Furthermore, commonly available knowledge through peer sharing can quickly address security issues and enhance the self-efficacy of employees. For example, a market researcher commented:

> *I expect to solve the problem in timely manner. Therefore, updating knowledge from surrounding colleagues is important and necessary to prevent risky situations. It is more on the spot support that formal IT channel cannot match*. (Market researcher 5.1)

A participant explained the benefit of having a local expert for security advice:

> *Because each department has a different policy – for example, a finance department cares more about personal trading policy than the marketing department – having an expert who has experience and knowledge about cyber security in our department is good idea, since they know what problems we usually face during work and we can trust them to ask.* (Compliance officer 4.2)

Another participant added how he paid more attention to security warnings from his colleagues than to general security updates from the IT department:

> *In my opinion, reminders from colleagues who have high security knowledge are more important to me, which will affect more on organisation's security effectiveness*. (Market researcher 5.1)

Some organisations did not conduct formal orientation for new staff members, who thus did not have efficacy to respond to security issues as expected. Therefore, direct senior staff members' advice can provide new users with specific and unique job-related security knowledge and requirements. Sharing knowledge between a designated local security expert and other colleagues is therefore a supplementary approach to enhance security knowledge of employees, which helped the participants to feel more competent in dealing with unknown security issues.

Table 2 summarises the key findings from the interviews regarding the effects on security information sharing methods on the participants' security practice.

Knowledge sharing methods	Current sharing practice	Effects on security awareness and practice
Email communication, instructor-led security training	Emails are commonly used as the main communication channel but are often ignored by employees because they are not customised to a specific audience. Security trainings are conducted only for new staff; follow-up sessions rarely happen. These methods can be complex and unengaging, and it is difficult to include contextualised security risks.	Provide good coverage of organisational security policies and procedures. Create initial necessity of security awareness, however, the effect does not last without regular repeat sessions. Less effective for on-going, urgent security updates.
Social media communication	No interviewed organisations had clear policies on the use of social media at work, though its use was popular among stock trading organisations. Suitable for organisations where staff members are using social media for work-related communications. Organisations can send quick updates, customise information to targeted recipients, and use more attractive contents. Members in the social group tend to know and trust each other to share security confidential information. Use of smart phones and social media applications are very common in Vietnam.	Attract immediate attention and caution from staff members because security risks are shared by someone they know. Effective in spreading urgent warnings because users use social applications more often than emails. Concern that confidential security information can easily spread out outside of organisational controls.
Local security experts	Senior staff members with good experience and knowledge of technology and applications used in respective departments can provide highly relevant and domain-specific advice. More convenient and timely to seek advice than through formal IT support channels.	Highly effective for timely, job-specific security advice when trust is important. Staff can respect and follow their advice. Provide effective feedback to novices or end-users without attending formal trainings. Can act as facilitator/whistle blower on security practices.

Table 2: Summary of study findings

6 Discussion

This study set out to explore how three methods of knowledge sharing – formal security training, social media, and local security experts (non-IT professional staff) – impacted employees' security practices. Thirty employees from eight organisations in finance, marketing and higher education in Ho Chi Minh City, Vietnam participated in eight in-depth focus group interviews. The findings contribute to both theoretical development in terms of self-efficacy and communication impact on security practice and practical steps that organisations can implement to support and encourage employees' information security compliance.

6.1 Theoretical contributions

Our study expands existing understandings of how self-efficacy can be developed and how its development can influence security practice. It does this through examining the impacts of

three knowledge sharing methods on participants' efforts to acquire security self-efficacy and to take recommended actions.

Rhee et al (2009) put forward and found support of three determinants of security self-efficacy – general computer experience, security breach experience, and general controllability – which in turn affect security practice (technology use and care behaviour) and efforts to strengthen security. This study elaborates further on these findings, exploring how such security breach experiences and the controllability of security risks can be acquired and built up through knowledge sharing through social media and local security experts. Knowledge obtained from these methods enhances employees' confidence to deal with security threats and motivates them to be committed to proper security practice. In addition, social media applications facilitate social group discussions, where people can comment and contribute to the information security problems in an informal setting, and modelling of appropriate behaviour is shared amongst peers. We posit that an employee's information security practices can be enhanced through learning in everyday activities from peers and local security experts. Given the complexity of security issues and the apparent lack of timely training, local security experts can also provide task-specific and timely advice in response to an immediate threat (Raineri & Paillé, 2016; Shafiq et al., 2013). As a point of close contact, local security experts can facilitate regular exchanges of best practices on similar issues and develop a communal approach to mitigating security challenges. Our study answers Rhee et al (2009)'s call to investigate the impact of indirect learning (learning from peers) and social persuasion (group discussion and sharing of proper practice) on security practice.

Furthermore, findings of this study confirm the arguments made in earlier studies that alternative communication methods are required to disseminate security information that can instil the importance of security practice and the needs to enhance self-efficacy (Willison et al., 2018). Alternatively, short and regular communications should complement annual training to maintain employees' ongoing security awareness (Barlow et al, 2018). We argue that different kinds of security information need different communication methods to attract users' attention and actions. Security policies and procedures can be shared via formal emails, and urgent security risk warnings should be delivered to specific user groups in media-rich and short messages via social media. Work-specific security issues can be initiated from local security experts who know the users and their specific requirements.

6.2 Practical implications

From a practical perspective, the findings suggest organisations should look at how security trainings and communication methods can be designed to attract employees' attention, justify their effort, enable employees to acquire necessary skills, and promote the notion of peer sharing of security issues and knowledge that may not be timely and adequately covered through formal channels. Security professionals should use a mix of communication channels, such as emails for general and periodical security updates and SMS and social media for urgent and critical risk updates. Particularly, our findings show that organisations can adopt social media tools to communicate security issues, taking advantage of their availability and accessibility on mobile devices (Kwahk & Park, 2016). While there are some caveats to this (e.g. public versus private sphere usage), people carry their mobile devices with them most of the time and disseminating urgent security messages through social media can therefore reach most people almost instantly.

Organisations should promote an open and trusted information security sharing culture and establish an infrastructure for employees to freely and conveniently share or report security risks at the workplace. Lacking a culture that encourages peer knowledge sharing can lead to higher risks, as found by Tamjidyamcholo et al. (2014). For example, learning about authentic security incidents from peers can have greater impacts on one's precautions in protecting organisational information assets (Furnell & Rajendran, 2012). However, to facilitate sensitive security information sharing, appropriate protocols need to be established providing guidance on what can be shared, in what formats, and on which channels. This study found employees considered sharing security topics among peers may not be appropriate due to a lack of trust and clear procedures.

Providing true-to-life security incidents in periodical security trainings is also important to demonstrate the real effects of security threats and taking recommended security measures (Willems & Meinel, 2012). As found by Rhee (2009), experience of previous security incidents can reduce one's perceived self-efficacy; hence those who have not experienced such incidents may underestimate the seriousness of security risks. Organisations should consider using gamification, simulation, and virtual scenarios to more effectively convey security information. Gamification approaches enable the creation of an active and collaborative working environment with higher motivation and enthusiasm, leading to better performance of employees (Burke, 2016).

Concomitant to concerns about the format of training is the timing of delivery. IT trainings should be organised for new hires and reinforced periodically. Lacking regular professional trainings is clearly evident in the organisations in this study, making the employees feel uninformed about the criticality of security knowledge and practice in their daily work.

7 Conclusion and future research

Maintaining security awareness is an important element in ensuring employees' compliance with security practice and an organisation's overall information security. Using in-depth interviews with users in eight organisations in Vietnam, our study explored how knowledge sharing through security trainings, social media, and local non-IT experts impacted employees' security awareness. While relatively narrow in focus, the study's findings contribute to both theoretical and practical aspects of improving employees' security practices. This study reaffirms the importance of developing self-efficacy through acquiring security awareness in users' security practices. It adds peer knowledge sharing as another dimension of self-efficacy, providing an additional way to improve security awareness. This study supports the role of sharing and giving security advice among peers, such as social groups, local experts, and professional IT staff.

For security practitioners, the study's findings highlight required changes in their training and communication methods to ensure employees' continued interest in and attention to security practice. It is important for organisations to develop robust knowledge sharing systems with supporting channels that utilise the latest mobile and social technologies and the expertise among employees. Employees normally take short-term precautions regarding security risks (e.g. are on high alert after a major security incident then ignore them soon afterwards). Through regular social media sharing and local experts, security risks and measures can be spread out to targeted audiences in a timely and personalised fashion. However, precautions need to be taken when sensitive security information is shared using social media.

This study has some limitations due to the nature of the research methodology. The small sample size of this study may not generalise the findings on a larger scale or establish a tested model of knowledge sharing methods and their impacts on security practice. The findings presented in this study mainly came from the employees' views toward security practice. Acquiring comparable responses from the security practitioners in each organisation would assess the practicality of new security communication channels, such as using social media for distributing security updates, which does carry additional risks.

Future studies should conduct quantitative surveys to validate the findings of this study and establish a model of knowledge sharing, for better replication of results across different organisational contexts. Such research would quantitatively ascertain the impacts of different information sharing methods on employees' security practice. Subsequently, more studies should investigate the impact of different antecedents of self-efficacy on users' security behaviour. Finally, it is important to acknowledge the inherent risks from sharing confidential information on social media. It is important to develop secure and private social media tools to protect the organisation. Further research could also investigate and validate the contradicting impacts of social media on employees' security behaviour and corporate confidentiality.

References

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3**,** 176-183. doi:10.4304/jait.3.3.176-183

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, 13**,** 195-201. doi:10.1016/j.istr.2008.10.006

Ashworth, P. (1999). ''Bracketing'' in phenomenology: Renouncing assumptions in hearing about student cheating, *International Journal of Qualitative Studies in Education*, 12(6), 707–721. doi: 10.1080/095183999235845

Barlow, J., Warkentin, M., Ormond, D. & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, 19**,** 689-715. doi:10.17705/1jais.00506

Brandl, D. (2012). 3 pillars of industrial cyber security. *Control Engineering*, 59, 8

Brennan, L. & Binney, W. (2010). Fear, guilt and shame appeals in social marketing. *Journal of Business Research*, 63**,** 140-146. doi:10.1016/j.jbusres.2009.02.006

Brown, J.S. & Duguid, P. (1999), Balancing act: How to capture knowledge without killing it, *Harvard Business Review*, 78, 3, 73-80

Bulgurcu, B., Cavusoglu., H. & Benbast, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security swareness, *MIS Quarterly*, 34, 3, 523-548. doi: 10.1016/j.cose.2020.101963

Burke, B. (2016). *Gamify: How gamification motivates people to do extraordinary things*, Routledge.

Chang, C. M., Hsu, M. H. & Lee, Y. J. (2015). Factors influencing knowledge-sharing behavior in virtual communities: A Longitudinal Investigation. *Information Systems Management,* 32**,** 331-340. doi:10.1080/10580530.2015.1080002

Cherdantseva, Y., Hilton, J., Rana, O. & Ivins, W. (2016). A multifaceted evaluation of the reference model of information assurance & security. *Computers & Security,* 63**,** 45-66. doi:10.1016/j.cose.2016.09.007

Clark, R. C. (2008). *Building expertise: Cognitive methods for training and performance improvement,* San Francisco, CA, John Wiley & Sons

Cilesiz, S. (2011). A phenomenological approach to experiences with technology: current state, promise, and future directions for research, *Education Tech Research Dev*, 59, 487–510. doi:10.1007/s11423-010-9173-2

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.), Thousand Oaks, CA: Sage.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computer & Security,* 32**,** 90-101. doi:10.1016/j.cose.2012.09.010

Cummings, J. N. (2004). Work groups, structural diversity, and knowledge sharing in a global organization. *Management Science,* 50**,** 352-364. doi:10.1287/mnsc.1030.0134

Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. *Archives of sexual behavior,* 41**,** 1319. doi:10.1007/s10508-012-0016-6

Feledi, D., Fenz, S. & Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report,* 17**,** 199-209. doi:10.1016/j.istr.2013.03.004

Furnell, S. & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security,* 2012**,** 12-15. doi:10.1016/s1361-3723(12)70053-2

Gupta, R. & Brooks, H. (2013). *Using social media for global security*, John Wiley & Sons

Hajli, N. & 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**,** 111-123. doi:10.1007/s10551-014-2346-x

Höne, K. & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security,* 21**,** 402-409. doi:10.1016/S0167-4048(02)00504-7

Hwang, Y. & Kim, D. J. (2007). Understanding affective commitment, collectivist culture, and social influence in relation to knowledge sharing in technology mediated learning. *IEEE Transactions on Professional Communication,* 50**,** 232-248. doi: 10.1109/TPC.2007.902664

Ipe, M. (2003), Knowledge sharing in organizations: A conceptual framework, *Human Resource Development Review*, 2, 4, 337-359. doi: 10.1177/1534484303257985

Jafari, N. N. & Charband, Y. (2016). Knowledge sharing mechanisms and techniques in project teams: Literature review, classification, and current trends. *Computers in Human Behavior,* 62**,** 730-742. doi:10.1016/j.chb.2016.05.003

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems Quarterly,* 34, 549-566. doi:10.2307/25750691

Juniper Research. (2017). *Cybercrime & the Internet of Threats* [Online]. Available: https://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats-2017 [Accessed 30 May 2018]

Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons,* 53**,** 59-68. doi:10.1016/j.bushor.2009.09.003

Kettinger, W. J., Li, Y., Davis, J. M. & 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**,** 59-75. doi:10.1057/ejis.2013.25

Khan, B., Alghathbar, K. S., Nabi, S. & Khan, M. (2011). Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management, 5, 10862-10868. doi:10.5897/AJBM11.067

Kwahk, K. Y. & 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**,** 826-839. doi: 10.1016/j.chb.2015.09.044

Liao, L. F. (2008). Impact of manager's social power on R&D employees' knowledge-sharing behaviour. *International Journal of Technology Management,* 41**,** 169-182. doi:10.1504/IJTM.2008.01599

Liu, D., Ji, Y. & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems,* 52**,** 95-107. doi:10.1016/j.dss.2011.05.007

Mallinder, J. & 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**,** 103. doi:Retrieved from: https://www.henrystewartpublications.com/jbcep

Mittal, S. & Dhar, R. L. (2015). Transformational leadership and employee creativity: mediating role of creative self-efficacy and moderating role of knowledge sharing. *Management Decision,* 53**,** 894-910. doi:10.1108/MD-07-2014-0464

Moustakas, C. 1994. *Phenomenological research methods*. Thousand Oaks, CA: Sage

Nonaka, I. & Takeuchi, H. (1995), *The knowledge creation company: how Japanese companies create the dynamics of innovation*, New York: Oxford University Press

Nonaka, I., Von Krogh, G. & Voelpel, S. (2006), Organizational knowledge creation theory: Evolutionary paths and future advances, *Organization Studies,* 27, 8, 1179-1208. doi: 10.1177/0170840606066312

Oh, S. (2012). The characteristics and motivations of health answerers for sharing information, knowledge, and experiences in online environments. *Journal of the American Society for Information Science and Technology,* 63**,** 543-557. doi:10.1002/asi.21676

Oostervink, N., Agterberg, M. & Huysman, M. (2016). Knowledge sharing on enterprise social media: Practices to cope with institutional complexity. *Journal of Computer-Mediated Communication,* 21**,** 156-176. doi:10.1111/jcc4.12153

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**,** 289-296. doi: 10.1007/s11416-017-0305-7

Pattabiraman, A., Srinivasan, S., Swaminathan, K. & Gupta, M. (2018). Fortifying corporate human wall: A literature review of security awareness and training. *Information Technology Risk Management and Compliance in Modern Organizations.* IGI Global

Pham, C. H., El-den, J. & Richardson, J. (2016). Stress-based security compliance model-An exploratory study. *Journal of Information and Computer Security,* 24**,** 326-347. doi:10.1108/ICS-10-2014-0067

Pham, C.H, Brennan, L and Furnell, S., (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications,* 46, 96-107. doi:10.1016/j.jisa.2019.03.012

Popovac, M. & Fine, P. (2018). An intervention using the Information-Motivation-Behavioral Skills Model: Tackling cyberaggression and cyberbullying in South African adolescents. *Reducing Cyberbullying in Schools: International Evidence-Based Best Practices***,** 225

Powell, J. (2018). An introduction to systems theory: from hard to soft systems thinking in the management of complex organizations. *Complexity and Healthcare Organization.* CRC Press

Puhakainen, P. & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly,* 34**,** 757–778. doi:10.2307/25750704

Raineri, N. & 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**,** 129-148. doi:10.1007/s10551-015-2548-x

Ramus, C. & Steger, U. (2000). The roles of supervisory support behaviors and environmental policy in employee "Ecoinitiatives" at leading-Eege European companies. *Academy of Management Journal,* 43**,** 605. doi:10.2307/1556357

Rhee, H.-S., Kim, C. & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28, 816-826. doi:10.1016/j.cose.2009.05.008

Rocha Flores, W., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security,* 43**,** 90-110. doi:10.1016/j.cose.2014.03.004

Safa, N. S. & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior,* 57**,** 442-451. doi: 10.1016/j.chb.2015.12.037

Safa, N. S., Von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security,* 56**,** 70-82. doi:10.1016/j.cose.2015.10.006

Schlienger, T. & Teufel, S. (2002). Information security culture. *Security in the Information Society*. Springer

Shafiq, M., Zia-ur-Rehman, D. M. & Rashid, M. (2013). Impact of compensation, training and development and supervisory support on organizational commitment. *Compensation & Benefits Review*, 45**,** 278-285. doi:10.1177/0886368713515965

Sindiren, E. & Ciylan, B. (2018). Privileged account management approach for preventing insider attacks. *International Journal of Computer Science and Network Security*, 18**,** 33-42

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 22**,** 42–75. doi:10.1108/IMCS-08-2012-0045

Sommestad, T., Karlzén, H. & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, 23**,** 200-217. doi:10.1108/ICS-04-2014-0025

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H. & Gholipour, R. (2013). Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. Computers & Education, 68, 223-232. doi:10.1016/j.compedu.2013.05.010

Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, 43**,** 19-34. doi:10.1016/j.cose.2014.02.010

Torres, H. G. & Gupta, S. (2018). The Misunderstood Link: Information Security Training Strategy

Wang, S. & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. *Human Resource Management Review*, 20**,** 115-131. doi:10.1016/j.hrmr.2009.10.001

Warkentin, M., Johnston, A. C. & 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**,** 267-284. doi:10.1057/ejis.2010.72

Wasko, M. M. & 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**,** 155-173. doi: 10.1016/S0963-8687(00)00045-7

Willems, C. & Meinel, C.(2012) Online assessment for hands-on cyber security training in a virtual lab. Global Engineering Education Conference (EDUCON), 2012 IEEE, 1-10

Willison, R., Warkentin, M. & Johnston, A. C. (2018). Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, 28, 266-293. doi:10.1111/isj.12129

Yang, J.-T. (2009). Individual attitudes to learning and sharing individual and organisational knowledge in the hospitality industry. *The Service Industries Journal*, 29**,** 1723-1743. doi:10.1080/02642060902793490

Zhang, S. & Costa, S. (2018). Mobile phone usage patterns, security concerns, and security practices of digital generation. *International Journal of Mobile Human Computer Interaction (IJMHCI)*, 10**,** 23-39.

Zhang, X., Pablos, P. O. d. & 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**,** 307-313. doi:10.1016/j.chb.2012.01.029

doi: https://doi.org/10.3127/ajis.v25i0.2177

Appendix A

Topic 1: Overall view of cyber security knowledge sharing

1. What do you think about the importance of updating cyber security knowledge in regard to your current job?
2. How often do you share information related to cyber security knowledge with your colleagues?
3. Who is the one that you usually share cyber security information or experience? Why?
4. What are your expectations from the IT teams (abilities, skills, enthusiasm and engagement)?

Topic 2: Effectiveness of knowledge sharing methods

1. Which method of communication makes you feel more interested in cyber security topics?
2. How can the company's spending on cyber security training programs affect your attitude/effort in putting effort to assist?
3. How cyber security training has been employed in your company? How do you think about its effectiveness?
4. How often do you use social media to share information with your colleagues at work? Do you usually share cyber security information to your colleagues via social media?
5. How do you think about the effectiveness of using social media on sharing cyber security information?
6. What do you think about staff sharing and support on cyber security topics? Would you be more interested if cyber security is shared/communicated through colleagues rather than a formal channel like security policies/IT policies?
7. What do you think about having someone who has rich knowledge of cyber security as one of your colleagues? Does it facilitate your willing to share cyber security information at work?
8. How do you think about the effectiveness of having a local IT expert (non-IT staff) as your colleagues on solving cyber security problem and improving your cyber security knowledge?