Who influences information security behaviours of young home computer users in Vietnam? An ego-centric network analysis approach

Duy Dang-Pham
School of Business IT and Logistics
RMIT University
Melbourne, Australia
Email: duy.dang@rmit.edu.au

Siddhi Pittayachawan
School of Business IT and Logistics
RMIT University
Melbourne, Australia
Email: siddhi.pittayachawan@rmit.edu.au

Vince Bruno
School of Business IT and Logistics
RMIT University
Melbourne, Australia
Email: vince.bruno@rmit.edu.au

Abstract

This study aims to explore the social roles of the people who can influence young home computer users (HCUs) in Vietnam, as well as the interactions that make those people influential. Since HCUs are considered the weakest link in the security chain and cyber-threats can attack organisation's information systems indirectly via these HCUs, it is therefore necessary to identify their sources of security influence for designing effective intervention. To this end, the ego-centric network analysis approach was employed to analyse the personal networks of security influence of 116 HCUs, comprising 548 influential sources in total. Close relationships such as family members, partners, friends, and colleagues were predominantly nominated as capable of influencing HCUs' security behaviours. Furthermore, these sources influence the HCUs by possessing the power bases of expert, reward, and coercive, as well as holding legitimate positions that make them influential.

Keywords

behavioural security, home computer user, social network analysis, egocentric network analysis

1 INTRODUCTION

Since the use of Internet is becoming more ubiquitous, home computer users are also exposed more to security and privacy threats (Kritzinger and Von Solms 2010). Home computer users (HCUs) can be defined as individual end-users who use the Internet at non-work locations and for personal purposes. As such, they are responsible for their own cyber-safety (Kritzinger and Von Solms 2010) and not protected by sophisticated protection, such as advanced firewall and professional IT supports, that would be usually implemented in work contexts. Moreover, it has been widely agreed that not all HCUs possess appropriate awareness of information security issues due to the lack of formal training (Howe et al. 2012; Kritzinger and Von Solms 2010). Without proper security awareness and protection, HCUs are extremely vulnerable to information security and privacy threats (Kritzinger and Von Solms 2010; Li and Siponen 2011).

Modern organisations cannot simply ignore the vulnerabilities of these HCUs, since their vulnerabilities and mistakes when using the Internet at non-work contexts can result in significant collateral damage (Anderson and Agarwal 2010; Dinev et al. 2009; Li and Siponen 2011; Liang and Xue 2010). This is due to the trending adoption of Bring-Your-Own-Device practice by many organisations that allow their employees to use personal devices (e.g. smartphones and laptops) for work purposes and bring work home, including confidential data (Dang et al. 2013; Liang and Xue 2010). As a result, careless Internet uses on the personal devices might have them infected by computer viruses that can steal or destroy the confidential data stored on these devices (Dang et al. 2013; Li and Siponen 2011; Liang and Xue 2010).

Improving HCUs' security awareness and their security behaviours appears to be the solution to compensate the lack of adequate technological protection and mitigate the cyber threats (Dinev et al. 2009; Li and Siponen 2011). To this end, prior studies have identified the contributing factors that influence the HCUs' security behaviours by empirically tested psychological and behavioural theories (e.g. Anderson and Agarwal, 2010; Lee et al., 2008; Zhang and McDowell, 2009). However, the number of studies focusing on end-users' information security at home remains overshadowed by those investigating the organisational context (Liang and Xue 2010). Furthermore, research adopting the traditional approach to investigate individualistic end-users overlooks the environmental catalysts that enable the positive effects on security behaviours that were identified by previous studies, thus limits the opportunities to develop effective interventions (Dang-Pham et al. 2014).

The objectives of this study are twofold. First, we employ social network analysis methods as a novel approach in the behavioural security field to examine the HCUs' personal networks that influence their security awareness and behaviours. As a result, this demonstrates the use of the ego-centric network research approach and provides directions for future studies. Second, we determine the specific types of interactions and social roles of these influential sources, from which practical recommendations about choosing the influential means to enhance HCUs' security awareness can be drawn. Ultimately, we aim to answer the following questions:

- RQ1: Who does influence home computer users' (HCUs) information security behaviours?
- RQ2: What are the interactions that make a person influential in information security?

2 LITERATURE REVIEW

2.1 Related work

Even though personal information security behaviours hold important roles in the whole security chain, the number of studies focusing on this research area remains overshadowed by those about workplace's security (Liang and Xue 2010). Amongst the HCUs' information security literature, a majority of them investigates the contributing factors that impact the HCUs' cognitive process that governs their security behaviours. For instance, Anderson and Agarwal (2010) found HCUs' concerns about security threats and self-efficacy can contribute to a positive attitude about personal security behaviours, which subsequently motivates the intention to perform the behaviours, together with other factors such as subjective norm and psychological ownership over own computer and the Internet. Similarly, Lee et al. (2008) and Liang and Xue (2010) found intention to perform personal security behaviours is motivated by the HCUs' perceptions of the security threats and coping measures, such as how much they feel vulnerable against the threats and how efficient the security practices could protect them from such threats. Most recently, (Dang et al. 2013) also found higher education students intend to perform BYOD-related security behaviours as they assess characteristics of the cyber-threats and security practices.

There is a growing number of recent behavioural security research focusing on the impacts of the security environment on security behaviours, which include the sources of security advice and influence. For instance, Warkentin et al. (2011) found a positive link between the employee's self-efficacy in information security and their access to learning sources such as situational support, verbal persuasion, and vicarious experience gained from job shadowing. Ifinedo (2014) found employees socialising with their colleagues can develop four types of bonds, which increase their perception of subjective norms and subsequently intention to comply with security policy. Likewise, in the other side of behavioural security research, various studies started to address the association between the workplace's features and the employee's tendency to commit malicious security behaviours. Examples of this trend include the extension of the Security Action Cycle which adds the "kinetic events" component (Willison and Warkentin 2013), and the research models that explain how work stress and perceived organisational injustice might lead to security violation (Dang 2014; Posey et al. 2011). In line with the increasing focus on the impacts of the security environment, Dang-Pham et al. (2014) proposed the use of social network analysis techniques to analyse the diffusion of malicious security behaviours in the workplace.

Several studies that aimed to identify the personal sources of HCUs' information security have been conducted primarily in Western contexts. For instance, Furnell et al. (2007) surveyed the population of UK residents about their information security awareness, and found a majority of them seek security advice from their friends, public websites, and IT professionals. Similarly, the sample of undergraduate students in the study of Aytes and Connolly (2004) reported to rely on friends and co-workers' security advice when making information security-related decisions, whereas half of this sample did not have any sources of advice. Furthermore, the recent literature review by Howe et al. (2012) revealed that the number of studies about the sources of information security advice remains limited and has not been updated since 10 years ago. While the important factors that positively influence HCUs' information security decision-making have been determined, there are fewer studies that address the sources of those factors. Without the knowledge of the catalysts that effectively deliver the contributing factors, it is challenging to design and conduct intervention and measures to practically improve HCUs' information security behaviours. Therefore, determining these sources of information security influence and advice becomes a crucial task (Howe et al. 2012).

2.2 Motivations and theoretical background

Our research objective about determining the sources of information security influence is similar to the concept of social capital. Social capital is a concept that has been studied widely in the sociology field, and its findings have informed studies about individual's behaviours, education, public health, economic development, and information systems, just to name a few (Adler and Kwon 2002). Across the different definitions of social capital, we found the external view of social capital most relevant and useful for guiding our study. This external view defines social capital as the links to actors and resources in a personal network that facilitate and explain the differential success amongst individuals (Adler and Kwon 2002). The salient social roles of network actors (e.g. acquaintances, friends, or family members) and the types of supports or resources provided by them are both core interests to social capital researchers (Borgatti et al. 2009, 2013). As such, prior studies determined the HCUs' sources of security influence have only revealed the social roles of the sources, while the interactions that result in such influence remain unexplored. In this research, we attempt to investigate further the types of interactions associated with the salient social roles, which influence the HCUs' security behaviours.

We rely on French and Raven's (1959) seminal theory of power bases to design our questionnaire and explore the potential types of interactions that make a person appear influential in information security to another. The updated version of this theory (Raven 2008) suggested that there are six types of influential power, including (1) informational, (2) reward, (3) coercive, (4) legitimate, (5) expert, and (6) referent power bases. Informational and expert types of power are similar in that a person can influence others through explaining them with persuasive reasoning (informational), or appear as possessing superior insights that the influenced agents put their faith into (expert) (Raven 2008). Provided that information security is often perceived as a technical area (Dang-Pham et al. 2014) and activities related to seeking security advice from knowledgeable colleagues have been documented by prior researches (e.g. Dourish et al. 2004; Warkentin et al. 2011; Wash 2010), we include the interactions related to teaching, explaining, and troubleshooting security in our questionnaire.

Reward and coercive power types that make a person influential are rather self-explanatory. However, it is worth elaborating that rewards and sanctions can be intangible (i.e. social) or tangible (e.g. money). For instance, sanctions have been consistently confirmed an important deterrence of security violations in the workplace context (Sommestad et al. 2014). Furthermore, Guo and Yuan (2012) found organisational sanctions fail to directly influence the employees' intention to violate security policy but

indirectly via workgroup and personal sanctions. In contrast, the effects of tangible and intangible rewards on security compliance still have inconsistent results (Dang et al. 2013; Siponen et al. 2014; Vance et al. 2012). Given these important effects of rewards and sanctions on information security behaviours, we also include them in our questionnaire.

Last but not least, individuals holding legitimate and referent positions can be influential to others (Raven 2008). Referent power involves the influential person is seen by the influenced agents as a role model, whom they admire and want to emulate beliefs and behaviours (Raven 2008). Such power could be caused by the social roles that the influential person holds, such as being a senior colleague at work or an elder family member. On the other hand, a person's legitimate status can be dictated by default by social norms and structures, or stem from the influenced agent's obligation to assist a helpless person or reciprocate a past favour (Raven 2008). Such dependent relationship can take place when a person feels the need to protect another's information security, such as exercising care when using the Internet at home to prevent the risk of virus infection in the home network (Dang et al. 2013; Li and Siponen 2011). Furthermore, there are more people co-sharing data and having access to another's data thanks to the rapid adoption of personal cloud storage. This subsequently results in the obligation to protect others' confidential data and also one own when co-sharing storage, especially when psychological ownership over personal computer and the Internet was confirmed as an influential factor of HCUs' security behaviours (Anderson and Agarwal 2010). As a consequence, we include these interactions in our questionnaire.

3 RESEARCH METHOD

3.1 Exploratory ego-centric network research approach

Despite its wide applications in other organisational behavioural fields, the use of social network analysis (SNA) approach in behavioural security field is still new (Dang-Pham et al. 2014). SNA methods are different from the traditional approach in that their main unit of analysis is the interactions and relationships between network actors, rather than their individualistic attributes (Otte and Rousseau 2002). As such, network researchers capitalise on this methodological feature and employ unique techniques to analyse the relational data and explore more in depth the environmental factors (Dang-Pham et al. 2014; Otte and Rousseau 2002). Network research primarily follows whole-network and ego-centric network research designs, between which the former has a boundary defined by the researchers (Borgatti et al. 2013). For instance, whole-network research might attempt to study the interactions and relationships between employees of the same organisation, whereas ego-centric network can be conducted by employing random sampling technique to collect data from a general population (Borgatti et al. 2013).

In addition to the fundamental concepts of nodes (i.e. network actors) and ties (i.e. the links between the actors), ego-centric network research focuses on analysing the personal networks of individual focal nodes (i.e. egos) and their neighbours (i.e. alters) (Borgatti et al. 2013). In fact, ego-centric network research contributes to the important concept of social capital, which refers to the link between one's possession of network resources such as social supports and their outcomes (Adler and Kwon 2002; Borgatti et al. 1998, 2009). Since our research questions focus on the sources of information security influence on the young HCUs' security behaviours, ego-centric network research is appropriate for such objectives.

3.2 Research context and data collection

As mentioned in the title of the research, our research is set in Vietnam–a developing country in South East Asia. Vietnam is currently ranked 13th in the world in terms of Internet penetration, with 52 per cent of the country's population are Internet users (Internet Live Stats 2016). However, the information security landscape in Vietnam has not yet reached its maturity. For instance, only 30 per cent of companies in Vietnam were found to have information security policies and measures in place (Vietnam MIC 2014). Worse still, Vietnam was ranked amongst the top five countries in the world where Internet users are threatned by computer viruses (Kaspersky 2014). As a result, there is an urgent need for identifying the sources of influence of HCUs' security behaviours and improving their awareness.

We designed our questionnaire to capture the salient social roles and security interactions identified in the literature review. The Vietnamese questionnaire was advertised on social media platforms such as Facebook and LinkedIn for three months to collect data from the general population. Besides capturing the ego's demographics (e.g. age and gender), the questionnaire asked the egos to nominate maximum seven people (alters) who can influence their information security behaviours. After the participants list

out the alters who can influence their information security behaviours, 19 probing questions verify the social roles (e.g. partner, family, friend, or colleague) and the security interactions that make them influential to the egos (e.g. teach security, share data with ego, or reward ego for security effort).

The limit of maximum seven nominations per ego was set as we believe it could help to significantly reduce the participants' stress in answering the questionnaire. This is due to each nominated alter has a set of 19 questions that aim to elaborate further the alters' social roles and interactions with the egos. Should we ask to nominate more than seven alters, the number of subsequent questions increases exponentially with the participants' stress. Furthermore, an empirical study conducted by Merluzzi and Burt (2013) suggested that five names would be sufficient for meaningful network analyses.

4 ANALYSIS & FINDINGS

4.1 Egos and alters' demographics

Our collected sample of 116 egos is young (mean age=23.84 years old; SD=4.532). The ratio of male and female respondents are considered balanced (male=47.4 per cent; female=52.6 per cent), which a majority of them rated their IT proficiency to be "intermediate" (49.1 per cent), followed by "advanced" (23.3 per cent), "novice" (22.4 per cent), and "expert" (5.2 per cent). These young HCUs tend to have their confidential data stored in personal computers (75.9 per cent), cloud storage (62.9 per cent), smartphones (60.3 per cent), USBs and portable drives (44.8 per cent), and social media such as Facebook (36.2 per cent). It is also interesting to find that personal cloud storage was considered the young HCUs' second popular choice for storing confidential data.

There is a total of 548 alters (or security influencers) who were nominated by our sample of 116 egos. Similar to the demographics of the egos, the gender ratio of these 548 alters is considered balanced (male=55.3 per cent; female=44.7 per cent). Most of these alters were reported to have completed Bachelor's degrees (71.5 per cent), followed by Master's (10.2 per cent), Diploma (9.1 per cent), under Diploma (6.0 per cent), and Ph.D. (3.1 per cent). A majority of them falls into the age range of 18–25 years old (58.2 per cent), followed by 26–35 (24.8 per cent), 36–45 (6.8 per cent), and the rest.

4.2 Social roles and interactions of information security influential sources

The information about the alters and their social roles to the egos help to answer research question 1. As explained in the research method section, our questionnaire directly asked the egos to identify maximum seven people who can influence their information security behaviours as well as social roles, thus allows the collection of this information. As seen in table 1, the most prevalent role that can influence one's information security behaviours is "friends", which accounts for 51.09 per cent (280 alters) in total. The second influential relationship role that influences our young Internet users are colleagues (14.78 per cent), followed by family (14.60 per cent). Surprisingly, there are more acquaintances nominated as being influential (7.12 per cent) than partners such as lovers and spouses (6.57 per cent), relatives (3.28 per cent), and seniors at work (2.55 per cent).

Table 1: Social roles of alters to egos

Social roles of alters to egos	# of alters	%
Friends	280	51.09
Colleagues	81	14.78
Family	80	14.60
Acquaintances	39	7.12
Partners	36	6.57
Relatives	18	3.28
Seniors	14	2.55

One potential reason that explains the influential statuses of these relationship roles could be due to the young Internet users in our sample spend more time to interact with their friends, as compared to other roles. Given that interaction plays a key role in interpersonal influences, such as via direct persuasion and indirect comparison (Leenders 2002), the level of interaction with a relationship role can determine how influential that role is. Since the mean age is 23.84 years old, there is also a high chance that these young Internet users do not work, hence receive less interaction and influence from professional roles such as colleagues and seniors.

To answer research question 2, we examine the interactions between the egos and alters. This information is summarised in table 2 below, and the interactions are categorised according to the types

of influential power (French and Raven 1959; Raven 2008) that they carry. Amongst the types of security supports or interactions that the egos receive, "Expert" is the most prevalent power which consists of people who can explain (296 alters) and teach information security matters (236 alters) to the egos. Consequently, each ego has access to a fair amount of people whom they consider knowledgeable in information security (204 alters). Moreover, the number of experts who can troubleshoot the ego's security issues (170 alters) is fewer than other types of experts.

Table 2: Security interactions from alters to egos

Power	Security interactions from alters to egos	# of alters	%
Expert	Can explain security threats to ego	296	54.01
	Can teach ego security matters	236	43.07
	Are considered knowledgeable in security by ego	204	37.23
	Can troubleshoot ego's security issues	170	31.02
Legitimate	Have access to ego's data	80	14.60
	Share confidential data with ego	103	18.80
	Are victims of cyber-attacks before	272	49.64
	Deserve protection by ego	299	54.56
Reward	Recognise ego's security effort	228	41.61
	Can reward ego for security effort	67	12.23
Coercive	Impose social sanction on ego's security negligence	195	35.58
	Can punish ego for neglecting security effort	65	11.86

Alters with "Legitimate" power are people whose social positions impact the ego's decisions to perform information security behaviours. In details, Raven (2008) explained that "legitimate" alters are influential thanks to the power recognised by social norm, the obligation of the ego to return a favour to the alter, or their dependence on the ego due to factors such as powerlessness. In our context, having access to the ego's confidential data or co-sharing data with the ego could grant the legitimate power that urges the ego to pay more attention to information security. Similarly, alters who are previous victim of cyber-attacks and deserve security protection by the ego for any reasons would be influential as well. Amongst the different types of "Legitimate" power, many alters were identified by egos as deserving their protection by default (299 alters) and being victim of cyber-attacks (272 alters). Some were nominated as sharing confidential data with the egos (103 alters) and having access to their data (80 alters).

Finally, "Reward" and "Coercive" power types rely on incentives and punishment to motivate behaviours (French and Raven 1959; Raven 2008). Consistent with the original theory, we categorised each of these power types into two sub-types, including the incentives and punishment that are tangible (e.g. monetary) and intangible (e.g. social recognition). Interestingly, the number of alters that can influence security by providing social recognition (228 alters) and sanction (195 alters) is higher than tangible reward (67 alters) and punishment (65 alters).

Our next analysis aims to determine the associations between the relationship roles and the types of interactions that result in security influence. One way to evaluate the associations between two variables is by computing their Jaccard distance, which is based on the co-occurrence of the variables across alters. The formula to calculate Jaccard distance is as followed:

$$d_j(A,B) = 1 - \frac{|A \cap B|}{|A \cup B|}$$

with A and B as two specific types of relationships about social roles or influential power. As the two types of relationships co-occur more, the numerator (i.e. the union of A and B) increases and thus makes the distance smaller. The use of Jaccard distances is a simple yet effective method for similarity comparison especially for network data (Hanneman and Riddle 2005). The Jaccard distances of the relationships are summarised in table 3.

Table 3: Jaccard distances between relationships (1: Explain threats; 2: Teach security; 3: Reward; 4: Recognition; 5: Punish; 6: Social sanction; 7: Victim; 8: Knowledgeable; 9: Share data; 10: Access data; 11: Need protection; 12: Troubleshoot)–smaller value means more association

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Partner	0.93	0.92	0.98	0.95	0.94	0.91	0.93	0.94	0.86	0.8	0.92	0.93
Family	0.87	0.9	0.88	0.86	0.96	0.9	0.86	0.91	0.86	0.9	0.82	0.91
Relative	0.96	0.96	0.95	0.97	0.96	0.96	0.98	0.97	0.95	0.96	0.96	0.96
Colleague	0.87	0.86	0.9	0.9	0.88	0.86	0.86	0.82	0.91	0.89	0.84	0.83
Senior	0.97	0.97	0.97	0.97	0.93	0.97	0.98	0.98	0.96	0.98	0.97	0.97
Friend	0.64	0.7	0.93	0.69	0.92	0.75	0.69	0.74	0.9	0.93	0.7	0.79
Acquaintance	0.95	0.94	0.95	0.94	0.97	0.97	0.93	0.94	0.99	0.98	0.96	0.97

The values in table 3 are coloured dark blues as they get smaller, whereas dark red values indicate a longer Jaccard distance (i.e. fewer co-occurrence) between two relationships. It may be tempting to interpret from the results that alters who are relatives, seniors, and acquaintances, are least capable of exerting influential power since they have the most number of red-coloured cells. Nevertheless, this is due to the numbers of relatives, seniors, and acquaintances nominated by the egos are smaller than other social roles (refer to table 1). The results in table 3 are therefore better used for understanding which influential power (columns) is most prevalent to a social role (rows). For this reason, it is important to take note that the cells in table 3 were also coloured according to their values as compared to those in the same row rather than across rows. As a result, a value of 0.8 may have a dark blue colour if it is the lowest in a certain row, but the same value of 0.8 may be coloured red if it is higher than the average in other rows.

Alters who are "partners" often have access to the ego's confidential data as well as co-share data with the ego. Such interactions were anticipated since sharing and accessing confidential data require a certain level of trust between people who are in an intimate relationship. Most alters who are "family members" were identified as deserving protection, while some can explain security, recognise or reward the ego's security efforts, and are victim of security incidents before. This result is consistent with prior studies about security behaviours in home context, where the HCUs' considerations about protecting the household network are commonly taken into account (Dang et al. 2013; Li and Siponen 2011). "Colleagues" were most recognised as knowledgeable in information security and being able to troubleshoot security issues and need the ego's protection. The most prominent influence that comes from "seniors" is tangible punishment on ego's security negligence. These interactions are understandable as colleagues could often be recognised as possessing professional expertise and have knowledge of the ego's work, thus were perceived as capable of providing relevant support. On the other hand, senior staff have formal authority which enables them to sanction the egos' negligence (Raven 2008). As consistent with the large number of nominations received, alters who are "friends" of egos are capable to exert many types of power, with notable ones include the ability to explain security threats, recognise ego's security efforts, and being victim of cyber-attacks. Last but not least, some "acquaintances" were recognised as knowledgeable in information security and victim of security attacks, as well as capable of teaching information security and recognising the ego's security efforts.

5 DISCUSSION & IMPLICATIONS

5.1 Discussion

Throughout our analysis, we have answered the two research questions stated in the introduction section. In particular, the young HCUs in our sample have their information security behaviours primarily influenced by their friends, followed by close relationships such as partners and family members. Interestingly, colleagues at work were found to influence these Internet users more than their relatives. We believe the time they spend with the alters on a regular basis governs whether an alter with a social role would be able to influence the ego's information security behaviours. For these young Internet users who are currently attending universities and working in entry/junior positions, it can be expected that their main sources of interactions would normally comprise friends who are fellow students and colleagues, and family members and partners who are outside of school and work life.

Despite being a significant issue (Howe et al. 2012), there is a lack of recent studies that identify the sources of security information or influence, especially in non-Western contexts. For instance, Aytes and Connolly (2004) surveyed 167 undergraduate students, of which 47 per cent reported not having any sources that can provide them information related to safe security practices. Amongst those who had information sources to seek advice from, 52 per cent of these sources are friends and co-workers.

Similarly, 41 per cent of 415 HCUs in the UK, who participated in a security awareness survey, reported to receive security advice from friends or relatives, followed by public websites (43 per cent), and IT professionals (Furnell et al. 2007). Our findings extracted from the Vietnamese/Asian sample extend prior results that friend-alters not only give security advice but also influence positively the HCUs' security behaviours. We further clarified that there were only a few relatives nominated for being influential, as compared to other close social roles such as family members and partners. Ng and Rahim (2005) empirically tested a security-related model, which was based on the Decomposed Theory of Planned Behaviour. They found that family and peers, as well as mass media, have positive effects on subjective norms that subsequently affected HCUs' intention to practice security. In this aspect, our findings mirror Ng and Rahim's (2005) empirical results.

Amongst the power bases discussed in French and Raven's (1959) theory, we detected a large number of alters who hold "Expert" power types and were nominated as influential towards the ego's information security behaviours. Since information security is still widely recognised by the end-users as a technical area (Dang-Pham et al. 2014), those who can explain and teach information security appear more convincing than others. Moreover, interactions such as delegating security responsibilities and seeking security advice from knowledgeable colleagues have been documented by prior studies in the workplace context (Dang-Pham et al. 2014; Dourish et al. 2004; Kirlappos et al. 2014; Warkentin et al. 2011). Our result supports this finding in personal or home context.

We found actors having access to others' data and co-sharing data with them can make these actors more influential in information security. Anderson and Agarwal (2010) found in their seminal study that psychological ownership over the Internet and own computer can motivate HCUs to perform security behaviours. Since ownership plays an important role in motivating security practices, those who share such ownership over the HCUs' confidential data can be reasonably expected to hold influential power. Furthermore, being recognised as a victim of prior security attacks was also suggested to make a person more influential to the others' security behaviours. Since past experience and consequences are confirmed stimuli of HCUs' information security behaviours (Howe et al. 2012; Lee et al. 2008), they would also consider these stimuli when assessing the potential influencers.

Rewards and punishment are common incentives that can modify beliefs and behaviours (Raven 2008). Moreover, social recognition and sanctions were nominated to have influential power towards our sample of young HCUs. Social sanction has been confirmed as a consistent deterrence of security violations, and in other cases, a motivation of security compliance (Sommestad et al. 2014). As a majority of security influential alters were nominated as capable of delivering social sanction on the ego's security negligence, our finding is consistent with prior studies in this aspect. In contrast, while existing research found that tangible sanctions can influence workplace's security behaviours as the employees realise the sanctions' severity and certainty (Sommestad et al. 2014), the alters nominated by the HCU-egos in our study were not reported to exert much of that influential power.

Tangible rewards for security efforts have been mentioned in research about organisational security management as a tactic to motivate compliance (Siponen et al. 2014), despite its empirical results were found to vary across work contexts (e.g. Dang et al. 2013; Sommestad et al. 2014; Vance et al. 2012). Our finding continues to support its influential role in the personal context, despite being ranked lower than social recognition. While intangible rewards such as peer's appreciation were not confirmed as a contributing factor of information security behaviours in the work context (Siponen et al. 2014), a number of our young HCUs identified being recognised as a reason why their information security behaviours are influenced by the people whom they interact with.

5.2 Implications

Having discussed and compared our findings with prior research, we found numerous practical and theoretical implications. First, we employed the ego-centric network analysis approach to analyse the interactions amongst HCUs rather than their individualistic attributes, as traditionally done by existing studies. This approach allows us to explore the different types of social roles and interactions that influence the HCUs' security behaviours, as well as determine their associations. As a consequence, future research investigating the effect of subjective norms may consider specifying the salient roles that can influence security behaviours, such as friends, family members, or partners, instead of asking generic questions that refer to important persons in general.

Furthermore, we encourage innovative uses of ego-network research approach to analyse the impacts of structural features on individual's security behaviours. For instance, the interrelationships between an ego's alters or neighbours (e.g. are friends to each other or co-share data) might put extra pressure on the ego to continuously exercise and learn security practices. This could be the ego's effort to create a

good image to their alters who know each other, or to increase the protection when the data is co-shared by many people. We have also collected but not yet analysed weighted relational data about the intensity of the interactions between egos and alters, such as frequency of communication, trustworthiness of security advice, and level of influence that each alter has on the egos. Network regression techniques can be applied in the next steps to predict the alters' influential statuses based on their social roles and security interactions. Gaining such understanding would further determine the specific salient social roles and interactions that influence end-users' security behaviours.

From a practical point of view, our findings contribute to intervention that aims to improve HCUs' security awareness and behaviours, especially by specifying the sources of security influence and the interactions that enable such influence. This would allow more effective investment of resources in the catalysts that can influence HCUs' security behaviours. From what we found about social recognition and sanctions being interactions that influence security behaviours, performing information security appears to have developed into a practice that yields social status. Educational institutions can promote the positive image of being proficient at information security to encourage learning and teaching security practices. Security influence was found to come from friends, family members, and partners, who not only spend more time with the young HCUs in daily life but can also provide them relevant and discreet advice about dealing with personal information security issues. Institutions can design and implement security awareness programs that involve the participation of people who hold those social roles, so to enhance the programs' positive influence over HCUs' security behaviours.

6 CONCLUSION

The sample of our study primarily consists of young HCUs in Vietnam, South East Asia. This subsequently limits our findings' generalisability to the samples similar to ours. It would be beneficial to conduct a survey that aims to cover a larger population, especially across cultural contexts for comparison purposes. Given the rapid Internet penetration and the increasing number of cyber-attacks that threaten organisations directly and indirectly, HCUs' information security behaviours and awareness must not be neglected (Anderson and Agarwal 2010; Dinev et al. 2009; Liang and Xue 2010). Nevertheless, educating and influencing HCUs' security behaviours are challenging due to the lack of professional support and infrastructure, as compared to the formal workplaces (Dang et al. 2013; Li and Siponen 2011).

Our exploratory study contributes to the intervention that aims to enhance HCUs' security practices, particularly by identifying the influential sources and their interactions that can influence HCUs' security behaviours. Gaining understanding of these sources and interactions would enable more efficient and effective targeted intervention. Furthermore, we demonstrated the empirical use of the ego-centric network research method, as a part of the social network analysis methodology, which has not yet been applied in behavioural security studies (Dang-Pham et al. 2014). As consistent with the suggested theoretical implications, we hope to stimulate novel ideas about using network analysis methods and encourage their adoption in the behavioural security field.

7 REFERENCES

Adler, P. S., and Kwon, S. 2002. "Social Capital: Prospects for a New Concept," *Academy of Management Review* (27:1), pp. 17–40 (doi: 10.2139/ssrn.979087).

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioural Intentions," *MIS Quarterly* (34:3), pp. 613–643.

Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices," *Journal of Organizational and End User Computing* (16:3), pp. 22–40 (doi: 10.4018/joeuc.2004070102).

Borgatti, S. P., Everett, M. G., and Johnson, J. C. 2013. *Analyzing Social Networks*, Sage Publications Ltd.

Borgatti, S. P., Jones, C., and Everett, M. G. 1998. "Network Measures of Social Capital," *Connections* (21:2), pp. 27–36.

Borgatti, S. P., Mehra, A., Brass, D. J., and Labianca, G. 2009. "Network Analysis in the Social Sciences," *Science* (323:April), pp. 892–896.

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2014. "Towards a complete understanding of information security misbehaviours: a proposal for future research with social network

approach," in *25th Australasian Conference on Information Systems (ACIS)*, Auckland, New Zealand.

Dang, D. P. T. 2014. "Predicting insider's malicious security behaviours: a General Strain Theory-based conceptual model," in *2014 International Conference on Information Resources Management (Conf-IRM 2014)*, Ho Chi Minh City, Vietnam.

Dang, D. P. T., Pittayachawan, S., and Nkhoma, M. Z. 2013. "Contextual difference and intention to perform information security behaviours against malware in a BYOD environment: A protection motivation theory approach," in *Australasian Conference on Information Systems (ACIS)*, Melbourne, Australia, pp. 4–6.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User behaviour towards protective information technologies: the role of national cultural differences," *Information Systems Journal* (19:4), pp. 391–412 (doi: 10.1111/j.1365-2575.2007.00289.x).

Dourish, P., Grinter, R. E., Delgado de la Flor, J., and Joseph, M. 2004. "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing* (8:6), pp. 391–401.

French, J. R. P., and Raven, B. 1959. "The bases of social power," in *Studies in Social Power*, pp. 150–167.

Furnell, S. M., Bryant, P., and Phippen, A. D. 2007. "Assessing the security perceptions of personal Internet users," *Computers and Security* (26:5), pp. 410–417 (doi: 10.1016/j.cose.2007.03.001).

Guo, K. H., and Yuan, Y. 2012. "The effects of multilevel sanctions on information security violations: A mediating model," *Information & Management* (49:6), Elsevier B.V., pp. 320–326.

Hanneman, R. A., and Riddle, M. 2005. *Introduction to social network methods*, Riverside, CA: University of California, Riverside.

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., and Byrne, Z. 2012. "The Psychology of Security for the Home Computer User," in *2012 IEEE Symposium on Security and Privacy*, Ieee, May, pp. 209–223 (doi: 10.1109/SP.2012.23).

Ifinedo, P. 2014. "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Information and Management* (51:1), Elsevier B.V., pp. 69–79 (doi: 10.1016/j.im.2013.10.001).

Internet Live Stats. 2016. "Internet Users by Country (2016)," (available at http://www.internetlivestats.com/internet-users-by-country/; retrieved July 5, 2016).

Kaspersky. 2014. "Kaspersky Security Bulletin 2014," (available at https://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014-EN.pdf).

Kirlappos, I., Parkin, S., and Sasse, M. A. 2014. "Learning from 'Shadow Security': Why understanding non-compliant behaviors provides the basis for effective security," in *USEC'14 Workshop on Usable Security*.

Kritzinger, E., and Von Solms, S. H. 2010. "Cyber security for home users: A new way of protection through awareness enforcement," *Computers and Security* (29:8), pp. 840–847 (doi: 10.1016/j.cose.2010.08.001).

Lee, D., Larose, R., and Rifon, N. 2008. "Keeping our network safe: a model of online protection behaviour," *Behaviour & Information Technology* (27:5), pp. 445–454.

Leenders, R. T. A. J. 2002. "Modeling social influence through network autocorrelation: constructing the weight matrix," *Social Networks* (24:1), pp. 21–47.

Li, Y., and Siponen, M. 2011. "A Call for Research on Home Users' Information Security Behaviour," in *15th Pacific Asia Conference on Information Systems (PACIS)*.

Liang, H., and Xue, Y. 2010. "Understanding security behaviors in personal computer usage: a threat avoidance perspective," *Journal of the Association for Information Systems* (11:7), pp. 394–413.

Merluzzi, J., and Burt, R. S. 2013. "How many names are enough? Identifying network effects with the least set of listed contacts," *Social Networks* (35:3), Elsevier B.V., pp. 331–337 (doi: 10.1016/j.socnet.2013.03.004).

Ng, B., and Rahim, M. 2005. "A Socio-Behavioral Study of Home Computer Users' Intention to

Practice Security.," in *PACIS*, pp. 234–247.

Otte, E., and Rousseau, R. 2002. "Social network analysis: a powerful strategy, also for the information sciences," *Journal of Information Science* (28:6), pp. 441–453 (doi: 10.1177/016555150202800601).

Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. 2011. "When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse," *Journal of Information System Security* (7:1), pp. 24–47.

Raven, B. H. 2008. "The bases of power and the power/interaction model of interpersonal influence," *Analyses of Social Issues and Public Policy* (8:1), pp. 1–22 (doi: 10.1111/j.1530-2415.2008.00159.x).

Siponen, M., Adam Mahmood, M., and Pahnila, S. 2014. "Employees' adherence to information security policies: An exploratory field study," *Information & Management* (51:2), Elsevier B.V., pp. 217–224.

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.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3–4), article, , pp. 190–198.

Vietnam MIC. 2014. "Vietnam Information and Data on Information and Communication Technology Whitebook 2014," Hanoi, Vietnam.

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), Nature Publishing Group, pp. 267–284 (doi: 10.1057/ejis.2010.72).

Wash, R. 2010. "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, New York, New York, USA: ACM Press.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1–20.

Zhang, L., and McDowell, W. C. 2009. "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords," *Journal of Internet Commerce* (8:3–4), pp. 180–197.