Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach

Duy Dang-Pham; Siddhi Pittayachawan; Vince Bruno
School of Business IT and Logistics
RMIT University, Melbourne
{duy.dang; siddhi.pittayachawan; vince.bruno}@rmit.edu.au

Abstract

Insider's intentional misbehaviours without the malicious intent to harm and security workarounds are emerging issues in information security behavioural field. To mitigate these insider's threats, prior research has been confirming many contributing factors of misbehaviours by focusing much on the cognition of employees as individual beings. Consequently, these studies' practical values are inevitably limited by the assumptions of their focus on individuals, which overlook the dynamic exchanges between organisational entities and collectives. From reviewing prior information security behavioural research and detecting their limitations, this paper introduces and proposes social network research as a new approach that would complement to the current body of knowledge. As a result, we discuss the potential directions of social network research and provide some potential research ideas that could be investigated using social network analysis techniques.

Keywords

information security behaviour, insider's threats, social network analysis, policy dissemination

INTRODUCTION

Today's organisations are prioritising their information security as they increase reliance on information systems (Bulgurcu et al. 2010). Furthermore, ensuring this protection has been considered as a sophisticated task since it requires a combination of secured practices from all parts of the organisation–including technological, behavioural, managerial, philosophical and organisational aspects (Crossler et al. 2013). It is common to find the current knowledge body of information security research comprises of multidisciplinary perspectives (Anderson and Moore 2009). Within that knowledge body, contemporary literature is focusing on the socio-organisational resources of the companies which concern individual and organisational perspectives (Bulgurcu et al. 2010). This focus is due to two reasons. First, it has been recognised that technological controls alone are not effective enough to protect information security (Lee and Lee 2002). Second, academics and practitioners realised the users as the weakest link in information security (Bulgurcu et al. 2010; Crossler et al. 2013; Dang et al. 2013). As a result, the information security behavioural subfield emerged and dedicated to study those socio-organisational factors (Crossler et al. 2013; Willison and Warkentin 2013). Nevertheless, information security behavioural research has just recently started to focus on why insider's misbehaviours occurred (Crossler et al. 2013; Warkentin and Willison 2009; Willison and Warkentin 2013). In particular, this paper will be focusing on those information security misbehaviours that are intentionally performed by insiders without malicious intent.

The term "insider" in information security behavioural research commonly refers to the users having access to the corporate information systems and knowledge of the organisational processes, which allow a wide range of information security behaviours including those that are disruptive, unethical or illegal (Willison and Warkentin 2013). Despite being dwarfed by the number of studies about compliance, a number of studies has been investigating why people performed noncompliant misbehaviours that are either intentionally or accidentally. While careless mistakes could be mainly explained by ignorance, we believe the deliberate misbehaviours with non-malicious intent (i.e. not aiming at harming the organisation) are much complicated and deserved more investigations. In fact, we noticed few prior studies have defined clearly the misbehaviours to be measured or examined (which are rather referred to as "security violation" in general), albeit such behaviours could vary in nature and the findings about them could have different implications. Notable examples of those who detailed the misbehaviours of interest include the works of (Guo and Yuan 2012; Guo et al. 2011). For instance, Guo and Yuan (2012) and Guo et al. (2011) defined their non-malicious security violations as deliberate and voluntary rule breaking, self-benefitting without the malicious intent to harm the organisation or individuals but could possibly cause damage or risk. While there is a current shortage of studies dedicating to investigate these particular misbehaviours, emerging research showed that the nature of this type of misbehaviours is even more complicated. For instance, Kirlappos et al. (2014) most recently discussed the term "shadow security" which describes the daily workarounds that are insecure but believed otherwise by the employees as their best attempt to protect the organisation's information security while maintaining self-convenient work practices. Regardless of their nature being intentional violations or clumsy workarounds, these misbehaviours could appear in the employee's daily tasks and hold dreadful yet hidden consequences if not receive proper attention. In fact, these types of misbehaviours were considered as one of the most serious insider's works in 2010 (Guo et al. 2011). The global information security survey by PwC (2014) reported that the number of security incidents increased 25% in 2013, among which 58% were believed to be performed by current (31%) or former employees (27%). Consistently, Verizon (2013) found an increase of more than 10% of reports regarding security breaches committed by insiders. In details, 14% of more than 47,000 incidents were performed deliberately by the internal actors (Verizon 2013). Indeed, research focusing on intentional misbehaviours with non-malicious intent has become even more vital to ensure information security of modern organisations.

We observed that prior research has been studying individual's cognition by focusing much on the individual as the fundamental unit of analysis while some theories such as General Deterrence Theory (Straub 1990) and Social Bonding Theory (Hirschi 1969) has been predominantly adopted. While we recognise the advance of these studies in determining the motivators and inhibitors of insider's misbehaviours, we contend that their implications are inevitably subject to certain paradigm assumptions, thereby limiting our understanding of the reality. This invites further investigations with a different perspective and motivates the writing of this article. The principal method of this research is a structured literature review that helps to confirm our observation regarding the theories and their assumptions being predominantly adopted to study the contributing factors of information security misbehaviours. Consequently, we proposed the social network approach as a new direction to move beyond the individuals and study the dynamics between them, so to address the paradigm assumptions being imposed on current studies. Ultimately, we aim at answering the research question and its sub-questions:

- RQ1: How social network approach can open up new directions for future research in information security behavioural field, especially about insider's misbehaviours?
- RQ2: What are the predominant paradigm assumptions (i.e. theoretical assumptions and fundamental unit of analysis) of prior studies?
- RQ3: What is social network approach and how it contributes to the current body of knowledge?

THE CONTRIBUTING FACTORS OF MISBEHAVIOURS

While we cannot claim our review is capable of covering all relevant studies, a structured approach has been taken to improve the rigour of our literature search (Webster and Watson 2002). Specifically, three researchers (i.e. the present authors) performed independent searches with relevant keywords (e.g. "antecedents AND information security misbehaviours"). Then, the results were gathered and analysed for common themes. The researchers then selected publications in leading journals and respected authors in the field to include in the literature review. Some examples of leading journals include Computers & Security, European Journal of Information Systems, Information Systems Research, Journal of Management Information Systems, and Information Management. Given the research question, the objective was to determine the contributing factors of information security behaviours, as well as the current underlying paradigm assumptions to be questioned for detecting new research opportunities. As found, a majority of the existing literature about information security misbehaviours focuses on individual as the fundamental unit of analysis and assumes that the perpetrator employs a rational choice approach in their decision-making process. Specifically, they weight the expected benefits and costs resulting from the behaviour, and their attitude or intention to perform the behaviour will then be reinforced or discouraged accordingly. This assumption is based on the common adoptions of criminology theories which we will discuss shortly. Two distinctive groups of the motivators and inhibitors of such misbehaviours—the extrinsic and intrinsic factors—are identified from the current body of knowledge.

Extrinsic Factors

To start with, General Deterrence Theory (GDT) has been the leading theoretical background which posits that the facets of *sanction* (i.e. certainty, severity and celerity) would serve as the disincentives of deviant acts and therefore deter the perpetrators from performing them (Straub 1990). The discouraging effect of sanction on insider's misbehaviours has been confirmed by many recent studies (e.g. Cheng et al., 2013; D'Arcy et al., 2009; Guo et al., 2011; Hu et al., 2011), despite some discrepancy of results caused by different methodological approaches (D'Arcy and Herath 2011). For instance, Hu et al. (2011) did not find sanction deter illegal and unethical violations such as transferring product designs, hacking and selling customers' data to competitors. As a result, they recommended employers to reduce the perceived benefits of violations and have better means to screen for employees with high moral belief and self-control, rather than relying on punishments alone. Similarly, Guo et al. (2011) argued upon the insignificant impact of sanction on the intentional, non-malicious and self-benefitting misbehaviours that sanction's effect was outweighed by the perceived extrinsic benefit. They noted that the actors in their scenarios were assumed to be aware of the policy, yet they still voluntarily violated it. The practical suggestion was to provide alternatives that meet both security and end-user objectives, rather than simply banning violations (Guo et al. 2011). In addition, they also found *perceived security risks* caused by the misbehaviours capable to discourage attitude and behavioural intention. Consequently, they advise security training to shift focus from IS security to business security and focus on educating the users about the risks of their behaviours. On the other hand, both D'Arcy et al. (2009) and Cheng et al. (2013) detected sanction's severity, but not certainty, could discourage intention to deliberately scan and look at confidential documents. Both studies suggested increasing the perceived severity and certainty of sanctions through security training program and policy as the extrinsic inhibitors of misbehaviours. However, it has also been supported that increased certainty of sanctions such as monitoring may violate the employee's privacy, which subsequently increases internal computer abuse and antisocial behaviour (Posey, Rebecca J Bennett, et al. 2011). Additionally, Posey et al. (2011a) adopted Causal Reasoning Theory to examine how the employee's causal attribution of organisational events would affect their perceived imbalance of environment and subsequently deviance behaviours. The study found that when the employees find it difficult to interpret the increased information security measures, it would result in a lack of attributed trust and lead to increased computer abuses. Employers were suggested to reduce the perceived uncertainty of the employees towards the organisation, as well as to be aware of the possibility of excessive monitoring's backfiring.

In contrast, extrinsic benefits were found to encourage the employees' attitude and intention to perform misbehaviours when the rational evaluation approach is taken. For example, Hu et al. (2011) detected that having *low self-control* could result in realising more the *intrinsic* and *extrinsic benefits*, therefore encouraged intention to commit computer misconduct. Interestingly, they detected that the extrinsic and materialistic gains displayed weaker impact on intention to commit abuses than the intrinsic, emotional gains such as excitement and thrill. Moreover, Guo et al. (2011) found *job performance's advantage* has positive impacts on both attitude and intention to perform misbehaviours. They interpreted such perceived advantage could be a desirable goal that the users would use misbehaviours as a legitimate mean to achieve such goal (Guo et al. 2011).

Intrinsic Factors

The most common intrinsic factors include the employee's own moral beliefs and the desire for social approval from the subjective norms of their peers. It is also worth noticing that subjective norms could serve as either a motivator or inhibitor of attitude/intention to perform misbehaviours. In one context, *subjective norms* was found to have positive influence on the employee's antisocial actions in the way that individuals with *low computer/security expertise* perceived compliance as irrelevant to their job and delegated security decision-making to supervisors or co-workers (Guo et al. 2011). They argued that the process in which workgroup norm affects employee's attitude was independent from their cost-benefit evaluation (i.e. job performance and security risks). Moreover, the employee was asserted to not even judge the morality of the misbehaviours as long as their actions are consistent with the norms (Guo et al. 2011). As a result, the research suggested training "power users" to serve as role models for other employees and increase overall security awareness. Consistently, research by Lee et al. (2004) detected positive impacts of *involvement* and *norm* on insider's abuse. In this case, a norm that advocates misbehaviours would serve as a motivator of the employee's attitude and intention to perform such behaviours.

On the other hand, Lee and Lee (2002) hypothesised that *attachment, involvement, commitment* and *belief* could influence the employee's attitude towards computer abuse, then subsequently affect behavioural intention. Their hypothesised model was also based on Social Bonding Theory (Hirschi 1969) in criminology, which assumed people as rational beings that have the tendency to commit crimes if low social control (consists of the four mentioned factors) failed to prevent them. In this sense, positive attitude towards misbehaviours is discouraged by the expected harms on co-workers (high attachment), concern of negating previous work efforts (high commitment) and moral belief about computer abuses as illegal acts (Lee and Lee 2002). Cheng et al. (2013) tested these hypotheses and found the discouraging effects of attachment, commitment, belief in conventional value system and subjective norms on intention to perform misbehaviours. Employers were further advised to improve the employees' attachment to their job and organisation as well as their loyalty to prevent abuses.

Regarding one's own *moral belief*, D'Arcy et al. (2009) found that moral commitment played a significant role in their model in influencing the individual's intention to perform misuses and controlling the effects of sanctions. Furthermore, moral commitment's discouraging effect was even stronger than sanction (D'Arcy et al. 2009). However, they contended that moral commitment would have less value in practice due to its variation depending on the individuals and therefore being difficult to control by organisations. More important, moral beliefs and social costs such as expected *shame* and *guilt* were introduced by D'Arcy and Devaraj (2012) in the form of informal sanctions (tested as social desirability), along with virtual status and employment level, as a theoretical advance of GDT. The study found informal sanctions to have strong influences in discouraging technology misuse intention, while virtual status slightly impacted the intention. It is also interesting to observe the insignificant effect of employment level, therefore assumed that both managers and non-managers staff would likely to have similar misuse intention (D'Arcy et al. 2009). However, they recognised that such insignificant result might be due to the lack of managers participated in the survey. In addition, *perceived identity match* was found to effectively discourage intention to perform misbehaviours both directly and indirectly mediated by attitude (Guo et al. 2011). It was interpreted that employees may refrain from the behavioural intention if the misbehaviours are perceived to contrast their professionalism, thus produces unfavourable attitude towards such behaviours.

Next Directions in Information Security Behavioural Research About Misbehaviours

Notably, there are two new research directions emerged from the field and received attention recently. First, there was a shift from examining individual and organisational factors as two separated entities to emphasising their interaction, suggested mostly by qualitative studies that investigated in-depth how the employees perceive the security controls. Perhaps one of the earliest studies which discussed such interaction between the employees and their environment was by Willison and Backhouse (2006). The study incorporated five criminology theories to advance a framework explaining how motivated offenders would find opportunities to perform abuses by gaining information from their routine activity and assessing the environment's controls. In this sense, the framework elaborates the dishonest employees' perspective in viewing and exploiting the systems risks caused by inadequate guardianship by security controls (Willison and Backhouse 2006). As a result, this research describes how a regular employee in specific circumstances perceives the attributes of the opportunity's structure, then exploits them and transforms into an offender.

Second, in line with this research direction was the extension of the seminal Security Cycle Action (SCA) (Straub and Welke 1998) by Willison and Warkentin (2013) to cover the employee-workplace interaction. By moving beyond the deterrence point of the SCA, they suggested that poor interaction between the employees and their workplace would produce disgruntlement, organisational injustice and motives as "pre-kinetic" events that reinforce behavioural intention to abuse. The importance of negative emotions in affecting insiders' misbehaviours was also emphasised. For instance, Baskerville et al. (2014) proposed an alternative of the framework discussed previously by Willison and Backhouse (2006), which consists of the emotion process involving appraisal of arousal, affect and action readiness. The modified framework also elaborated the regulation (internal and external) process, the offender's concerns about relevant events that trigger negative emotions, as well as the action availability according to the organisation's liberty (i.e. freedom of movement) and physical environment. Most recently, Dang (2014) proposed a conceptual model describing the contributing effects of work strains on the employees' perceived organisational injustice, which subsequently results in anger and reinforces the insider's abuses.

In summary, the discussed literature so far has made clear that the positive attitude towards misbehaviours and their behavioural intention receive influences from a range of organisational and individual factors. In details, the perpetrators were asserted to be motivated by materialistic gains such as job performance (Guo et al. 2011; Hu et al. 2011), or negative emotions which result in expressive actions (Baskerville et al. 2014; Dang 2014; Posey, Rebecca J Bennett, et al. 2011; Willison and Warkentin 2013), or they just simply want to follow the norms that encourage the misbehaviours (Cheng et al. 2013; Lee et al. 2004). In some cases, the motivated offenders evaluate the situations to find their opportunities and act accordingly (Baskerville et al. 2014; Willison and Backhouse 2006). In turn, security managers could use the sanction's effects of formal controls to deter misbehaviours (Cheng et al., 2013; D'Arcy et al., 2009; Guo et al., 2011; Hu et al., 2011; Lee et al., 2004), which at the same time could be harmful by creating even more security risks if perceived as excessive by the employees. The only disincentive that has been consistently found effective was the individual's moral belief (D'Arcy and Devaraj 2012; D'Arcy et al. 2009) that discourages the misbehaviours. Nevertheless, personal moral belief was suggested to vary among individuals and organisations may find it difficult to shape varied beliefs, therefore holds little practical values.

CURRENT GAPS AND OPPORTUNITIES FOR A NEW APPROACH

Other Than "Bad Apples" & "Bad Barrels"–The Patterns and Dynamics in Between

There was a seminal article about unethical organisational behaviours by Brass et al. (1998) which described the individuals as "apples" inside their "barrels" i.e. organisation. This article presented two points of view regarding the cause of unethical organisational behaviours: whether it was due to the "rotten apples" that spoil the barrels (individual's attributes that influence organisational unethical behaviours), or it was the "bad barrels" that damage the apples within (organisation’s culture and norms that promote unethical behaviours). Nevertheless, this dichotomy of bad apples and bad barrels have been abandoned by researchers since its approach was unable to capture the complexity of the interaction between the individuals and their organisations when it comes to making unethical or ethical decisions (Brass et al. 1998). Come back to the information security issues of intentional violations and harmful workarounds, it could be observed that a majority of the prior research reviewed in this article has been focusing much on the “apples” and the remaining few briefly addressed the role of the “barrels”. While their finding provided a wealth of knowledge about what does and does not influence misbehaviours, these studies have certain assumptions and gaps that we found interesting to develop knowledge upon.

For instance, the major extrinsic inhibitor of misbehaviours, sanction, has its formal deterrent effect depends on the dissemination of information security policy. Accordingly, General Deterrence Theory assumes the perpetrators are aware of and respond to the punishment associated with effect policing (Straub 1990). As a result, it could be argued that the confirmed findings about the effects of sanctions are subject to the policy being known. Nevertheless, information security policy is hardly read or referred to by the employees (Wood 2000), not to mention that a security policy may not even be formally available in some organisations. Likewise, we contend that the poor dissemination of information and knowledge may also occur in how subjective norms and social bonding are realised and perceived by the employees. For instance, there could be solitary individuals or groups, due to constraints or deliberate refusal to participate, that do not receive any influences from any social or political influences, thereby rendering the effects of norms and bonding ineffective.

More importantly, recent studies have shown that security are collective information practices of risk, trust and morality (Dourish and Anderson 2006). It was emphasised that the individuals’ different perceptions of risk should be examined “relative to social structure” and they interpret risk according to their positions in such structures (Dourish and Anderson 2006 p. 330). Similarly, the workarounds or “shadow security” behaviours also resulted from the employees’ interpretations of risks that are different from the security managers’ expectations (Kirlappos et al. 2014). On the other hands, trust and morality are also factors that have been included in information security behavioural studies. In particular, Kirlappos et al. (2013) argued that centralised policy may not fit with local and situational events that demand greater flexibility to cope with information security risks, thereby suggesting the employees to be trusted in making own decisions to mitigate the perceived risks. Interestingly, it was found that the employees tend to delegate their responsibility when making information security decisions, and trust is a form of investment required by the different kinds of delegation (Dourish et al. 2004). More specifically, they found that the employees delegated security to technologies, knowledgeable acquaintances, organisations or institutions that they believe as trustworthy. Moreover, the delegated individuals are even referred to as the guarantor of the security responsibility even if they leave the scene (Dourish et al. 2004). Similarly, Kirlappos et al. (2014) also reported this group-based decision making process when investigating how “shadow security” behaviours were created and performed within workgroups.

Those findings inspired the research idea that focuses on the holistic social structure that transmits information relating to information security within the organisation, to be used by employees with attributes and decisions relational to relevant entities such as work groups, policies and technologies. Such idea is similar to but also different from the next direction of information security behavioural research that we discussed previously. On one hand, Willison and Warkentin (2013) suggested studying the impacts of factors created by the workplace-employee’s interaction on individuals’ misbehaviours. Consequently, potential knowledge generated from this direction would contribute to the current understanding about the bad apples’ cognitions and behaviours as individual beings. On the other hand, we propose to examine the patterns of the relationships and the interactional activities between the “apples”, and how the individual or collective information security decisions would be influenced by these patterns and activities. Based on the recent findings presented previously about intentional misbehaviours without malicious intent and “shadow security”/workarounds, we found that risk, trust, responsibility, morality, as well as artefacts such as policy and security controls hold crucial influences on such misbehaviours. More importantly, they could be created, interpreted, shared and delegated by the employees among organisational collectives, thereby influencing information security decisions. As a consequence, we suggest the potential social network research approach in information security behavioural field and particularly how social network analysis can be a useful method to study the mentioned aspects.

A Brief Introduction About Social Network Research Approach

By adopting the social network research approach, researchers shift their attention away from the individuals and aim at generating knowledge that are more relational, contextual and systemic (Borgatti and Foster 2003). Supporting this research approach is the use of social network analysis (SNA) as a research method for capturing and measuring the features of networks’ social structure. SNA has been increasingly applied in management and organisational studies to investigate the beliefs and behaviours of people as interconnected beings that are influenced by the relationships patterns among them within the organisational and social systems (Zack 2000). In contrast, as far as we know there has been only the recent work of Yoo and Lawrence Sanders (2013) in information security behavioural field that used SNA to explore security compliance at group level. Similarly, in the coming paragraphs we will propose ideas based on the major streams of social network research in organisational and management studies, rather than provide a technical how-to guide, so to exploit the rich applications of SNA and extend this new research direction in information security behavioural field. Among the literature reviews on doing social network research, we found the recent work by Carpenter et al. (2012) very useful in providing a comprehensive and systematic guide. Specifically, they identified two main schemes of social network research namely “social capital” and “network development”, which both aim at studying interpersonal (i.e. actors are people) and inter-organisational (i.e. actors are firms or their representatives) levels. In our context of employees’ information security misbehaviours, investigations at the interpersonal level would be most fitting.

The schemes of research is categorised according to the social network’s role and the research’s objectives (Carpenter et al. 2012). On one hand, social capital research is interested in analysing the networks as causes or predictors of their consequences (on node- or group-level). In details, social capital is referred to as the utility and benefits that the participants receive from the networks such as power and influence, access to resources, increased performance and creativity, and such social capital could be achieved by “network application” and “network structure” (Carpenter et al. 2012). The network application construct measures how effectively the actors can use the resources flowing through their possessed ties to influence the different outcomes, whereas network structure analyses the structural patterns and features of the actors’ participated networks, so to determine the influences on the received social capital. On the other hand, network development research concerned with the changes and evolution of networks’ formation due to two major forces, including ongoing network structure’s opportunities and intentional shaping by organisation’s inducements (Carpenter et al. 2012). For instance, network structure predictors can be the basic features of networks such as ties, triads and nodes that result in the routines of how networks change, as in how new ties could emerge between firms and their former partners, or a weak tie could break down a triad of acquaintances which it belongs to (Carpenter et al. 2012). Besides the routine transformations of network according to its current features, actors can also purposely shape the networks via homophily and instrumentality. Homophily describes the situation when people tend to connect with those of similar attributes, thus demonstrates that network structure can be influenced by active matching of demographics, personalities or jobs’ natures. Instrumentality refers to the actors’ perceived values of the networks, influenced by their demands and resources available. Consequently, non-network precursors such as resource demands, environmental pressures and reputation have been examined for their predicting effects on social networks by prior research (Carpenter et al. 2012). The research schemes and their respective predictors/predicted consequences can be summarised in Table 1.

Table 1: Social network research at interpersonal level (adapted from Carpenter et al., 2012)

Schemes	Predictors	Predicted consequences
Social capital research	*Network application:* utilisation of flowing resources. *Network structure:* patterns and features of actor’s social networks.	*Social capital benefits* (e.g. power, influence, access to resources, performance etc.).
Network development research	*Opportunities/network structure:* nodes and network level, less dyadic level. *Actor’s purposeful inducements/non-network constructs:* homophily and instrumentality (values of networks determined by actors’ demands).	*Network structure:* nodes and network level, less dyadic level. *Network application:* mainly network possession.

Applying Social Network Research in Information Security Behavioural Field

Social network research can be “applied” or “basic”, and each direction has its own analysis goal (Borgatti et al. 2013). Accordingly, *applied social network research* aims at calculating the metrics that reflect the networks’ structure, which can be interpreted by network analysts so to devise appropriate follow-up actions. Some examples of these applied studies include identifying key persons by their centrality in the network to leverage diffusion of innovative practices to these individuals, or to determine the isolated employees in the firm and provide interventions so that they can be more connected. In harmony with the applied type is the *basic research* which aims at understanding the causal process between the predicting conditions and their subsequent outcomes. In other words, basic social network research confirmed the causal phenomena so that the applied ones can base on such to make effective decisions given the networks at hands. Borgatti et al. (2013, p. 6) described two types of theories that basic social network research seeks including “network theories of __” and “__ theories of networks”, whereas the researchers can fill in the blanks with their variables of interest. More specifically, researchers can measure the features of the actors’ position in the network and use those features to predict, for example, their political influence within the firm. As a consequence, this would result in the “network theory of political influence”. On the other hand, there is the case when an independent variable such as political views could be used to predict how people having the common opinions would become each other’s friends. This in turn leads to the “common political views theory of network tie formulation”. While the categorisation in Table 1 provides a brief yet systematic understanding about social network research’s capabilities, the discussed analysis goals further shape our ideas of how to apply SNA to address information security behavioural research questions. In the coming paragraphs, we will discuss some potential research ideas about information security misbehaviours that fall into the categories of applied and basic social network research, particularly the uses of network variables as predictors of security-related factors. The stream of basic research that uses network variables as predicted outcomes is not included in our discussions because their theoretical contributions focus more on network areas, therefore being out of this paper’s scope which is information security misbehaviours.

Applied social network research

If the spread of misbehaviours or workarounds among individuals was a confirmed phenomenon, it would be desirable to investigate where it starts and which routes allow or accelerate the spreading process so that interventions can be made. One possible approach, which has been done quite commonly in information security behavioural field, is to provide the participants vignettes of security violations and measure their behavioural intention. At the same time, researchers can build sociogram that describes advice networks of the employees, especially when they seek each other for information security-related advice or induction, as mentioned in the study of Kirlappos et al. (2014). By combining these data, it would be possible to trace back the key employees/sources that spread the misbeliefs about information security. Furthermore, quasi-experiment research can also be conducted to monitor how interventions would change the networks’ features as well as the individuals’ characteristics. For instance, by knowing the sources of information security behaviours and their influential networks, security managers can conduct targeted-trainings aiming at those individuals with the hope that they would disseminate the recommended practices, and then generate another sociogram after a while to measure the changes and assess their effectiveness.

Basic social network research

Prior and current research has confirmed many contributing factors that influence behavioural intention and attitude towards information security misbehaviours, and we expect that studying the networks’ features as predictors of those factors would bring complementary values. For instance, formal and informal sanctions have been consistently found to produce discouraging effect on intention to perform misbehaviours, but its effectiveness is tied to the assumption that the sanctions are recognised by the employees. By using SNA, it could reveal how formulations and characteristics of ties and nodes’ positions would contribute to the evenly distributed awareness about sanctions, therefore improves their practical applications. Similarly, this approach can also be applied to other important inhibitors and motivators of misbehaviours introduced previously such as subjective norms, social bonding, and intrinsic and extrinsic benefits.

Moreover, employees were found to make information security decisions based on their interpretations of risks and delegate security to other entities based on their trustworthiness (Dourish and Anderson 2006; Dourish et al. 2004). In addition, work groups and teams develop their own security micro-cultures that mediate and permit misbehaviours to happen (Kirlappos et al. 2014). Conveniently, such joint actions and collaborative processes are the main analysis targets of SNA techniques, especially via studying bridging and bonding ties. While bridging ties allow access to resources and link different subgroups within a network together, bonding ties play crucial roles in fostering trust and reciprocity within the groups, thereby making them more cohesive (Bodin and Crona 2009). In this case, adopting SNA to measure the levels of trust investment between the employees and their reachability to relevant resources (e.g. peers, technologies, prescribed procedures and solutions) would yield interesting findings. For example, we could test the relationships between networks’ structure and security decisions to answer questions e.g. would individuals possessing many connections receive more security delegations since they are more reachable, and whether high centrality would result in trust investment as well? Furthermore, we can also identify the key entities in the security decision-making process by looking at the attributes and answering questions e.g. what are the common attributes of trustworthy entities that individuals seek security advice from or delegate their security to? This would allow exploitation of these key entities’ influences or removal of the root causes of misbehaviours.

It needs to be emphasised that SNA techniques are versatile and have many metrics which can be used to study the impacts of networks’ dynamics and structural features on misbehaviours, while we have just discussed a modest amount of potential research directions and applications. More importantly, the suggested social network approaches (i.e. applied and basic; social capital and network development) are not only closely related to each other but also to prior research in information security behavioural field, particularly in terms of complimenting each other with research findings. The links between social network research directions and prior research, as well as between the multiple directions within the social network approach, are discussed throughout our study and illustrated in Figure 1 below.

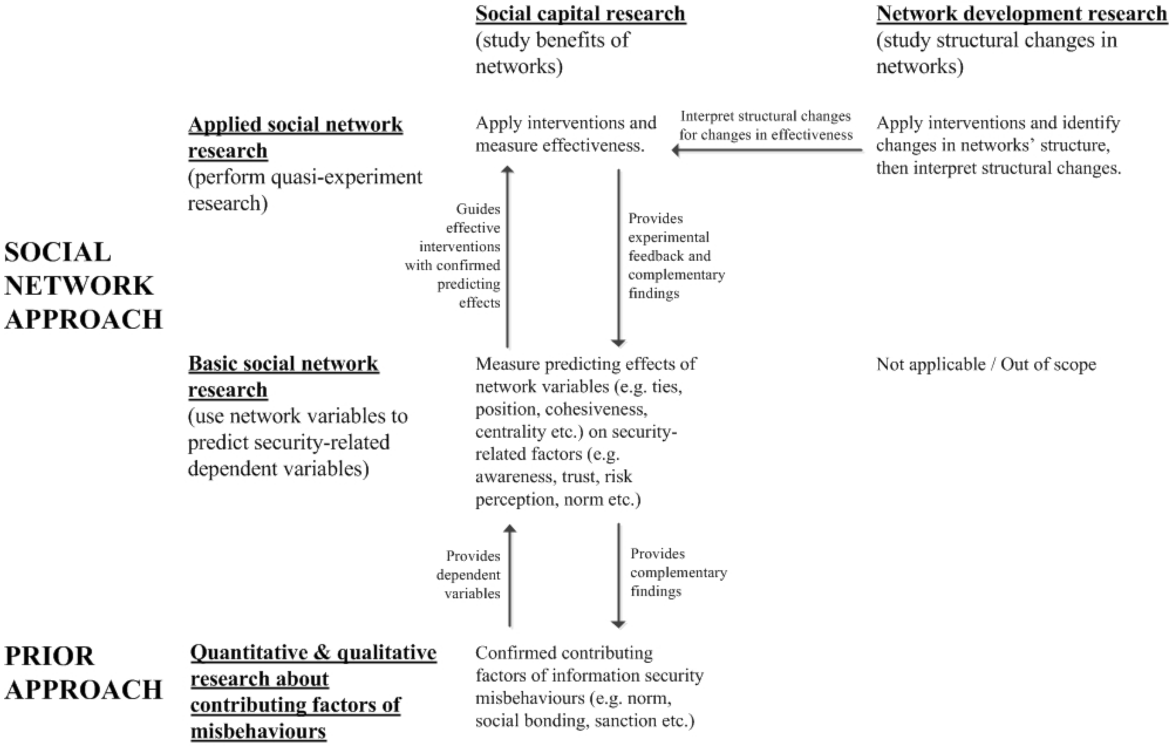
Social capital research
(study benefits of networks)
Network development research
(study structural changes in networks)
Applied social network research
(perform quasi-experiment research)
Apply interventions and measure effectiveness.
Interpret structural changes for changes in effectiveness
Apply interventions and identify changes in networks' structure, then interpret structural changes.
SOCIAL NETWORK APPROACH
Guides effective interventions with confirmed predicting effects
Provides experimental feedback and complementary findings
Basic social network research
(use network variables to predict security-related dependent variables)
Measure predicting effects of network variables (e.g. ties, position, cohesiveness, centrality etc.) on security-related factors (e.g. awareness, trust, risk perception, norm etc.)
Not applicable / Out of scope
Provides dependent variables
Provides complementary findings
PRIOR APPROACH
Quantitative & qualitative research about contributing factors of misbehaviours
Confirmed contributing factors of information security misbehaviours (e.g. norm, social bonding, sanction etc.)

Figure 1: The links between social network approach (including its directions) and prior research

It is crucial to acknowledge the difficulties of conducting social network research. Since the findings are derived from the networks and their nodes, they could be affected by omission errors as a result of poor data collection (Borgatti et al. 2013). In analysing the networks, these authors warn edge/node attribution errors can mislead interpretations of network data (e.g. assume connection between two students by observing them attend the same classes, but in fact they do not hang out together), and suggest triangulation of other relational data. Finally, interviewee's burden while answering social network questionnaire must be considered, especially when the questions are intrusive (e.g. name specific people and rank their importance), exhaustive (e.g. pick five out of 500 employees as the most approachable ones), or prone to retrospective error (e.g. who did you interact with in the company's dinner last night) (Borgatti et al. 2013). While the holistic focus of this approach which tends to emphasise more on the network's surface could be complemented by existing research that studied in-depth each individual of the network, the discussed difficulties and the method's technical nature could be the main reasons that limit the choice of using this approach in information security behavioural field.

CONCLUSION

It has been widely recognised that information security threats coming from inside of the firms are equivalently devastating to, if not even greater than, external attacks since the perpetrators have the necessary knowledge and rightful access to the organisational systems (Dang 2014). Worse still, misbehaviours without the malicious intent to harm or clumsy workarounds caused by information security misbeliefs are quite common and can be spread stealthy within the workplace (Kirlappos et al. 2014). Prior and current research has been producing a great wealth of knowledge regarding the contributing factors of those misbehaviours while focusing much on the cognition of employees as individual beings. However, findings from the current theory-testing approach have their practical values inevitably limited by the theories' assumptions which overlook the dynamic interaction between organisational entities and collectives in the reality.

As a consequence, we propose a set of social network research directions as a promising approach for future studies in information security behavioural field. In particular, employing social network analysis techniques allows researchers to explore further the relationships between the confirmed contributing factors of misbehaviours and the organisational/individual networks, including the networks' structural features as well as the dynamics of exchange activities between organisational entities. We believe the social network approach not only complements the current understanding about information security misbehaviours but also produces new knowledge in aspects such as dissemination of information security policy, measuring discrepancy of security goals and expectations, formation and transformation of security climates and sub-cultures, just to name a few. This paper aims to be one of the firsts that advocates the adoption of social network analysis techniques in information security behavioural field, and we look forward to seeing interesting findings emerge from future research following this approach.

REFERENCES

Anderson, R., and Moore, T. 2009. "Information security: where computer science, economics and psychology meet.," in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, (Vol. 367) , July 13, pp. 2717–2727.

Baskerville, R., Park, E., and Kim, J. 2014. "An emote opportunity model of computer abuse," *Information Technology & People* (27.2), pp. 1–31.

Bodin, Ö., and Crona, B. I. 2009. "The role of social networks in natural resource governance: What relational patterns make a difference?," *Global Environmental Change* (19:3), pp. 366–374.

Borgatti, S., and Foster, P. 2003. "The network paradigm in organizational research: A review and typology," *Journal of management* (29:6), pp. 991–1013.

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

Brass, D., Butterfield, K., and Skaggs, B. 1998. "Relationships and unethical behavior: A social network perspective," *Academy of Management Review* (23:1), pp. 14–31.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study on rationality-based beliefs and information security awareness," *MIS quarterly* (34:3), pp. 523–548.

Carpenter, M. a., Li, M., and Jiang, H. 2012. "Social Network Research in Organizational Contexts: A Systematic Review of Methodological Issues and Choices," *Journal of Management* (38:4), pp. 1328–1361.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Computers & Security* (39), pp. 447–459.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (32), pp. 90–101.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091–1124.

D'Arcy, J., and Herath, T. 2011. "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings," *European Journal of Information Systems* (20:6), pp. 643–658.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

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.

Dourish, P., and Anderson, K. 2006. "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena," *Human–Computer Interaction* (21:3), pp. 319–342.

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.

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.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model,” *Journal of Management Information Systems* (28:2), pp. 203–236.

Hirschi, T. 1969. *Causes of delinquency*, University of California, Berkeley.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. “Does deterrence work in reducing information security policy abuse by employees?,” *Communications of the ACM* (54:6), p. 54.

Kirlappos, I., Beautement, A., and Sasse, M. A. 2013. “‘Comply or Die’ Is Dead: Long Live Security-Aware Principal Agents The Need for Information Security,” in *Financial Cryptography and Data Security*, Springer Berlin Heidelberg, pp. 70–82.

Kirlappos, I., Parkin, S., and Sasse, M. A. 2014. “Learning from ‘Shadow Security’: Why understanding non-compliant behaviors provides the basis for effective security,” .

Lee, J., and Lee, Y. 2002. “A holistic model of computer abuse within organizations,” *Information Management & Computer Security* (10:2), pp. 57–63.

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. “An integrative model of computer abuse based on social control and general deterrence theories,” *Information & Management* (41:6), pp. 707–718.

Posey, C., Bennett, R. J., and Roberts, T. L. 2011. “Understanding the mindset of the abusive insider: An examination of insiders’ causal reasoning following internal security changes,” *Computers & Security* (30:6-7)Elsevier Ltd, pp. 486–497.

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.

PwC. 2014. “Key findings from The Global State of Information Security ® Survey 2014,” .

Straub, D. D. W., and Welke, R. J. R. 1998. “Coping with systems risk: security planning models for management decision making,” *MIS Quarterly* (22:4), pp. 441–469.

Straub, D. W. 1990. “Effective IS Security: An Empirical Study,” *Information Systems Research* (1:3), pp. 255–276.

Verizon. 2013. “2013 Data Breach Investigations Report,” .

Warkentin, M., and Willison, R. 2009. “Behavioral and policy issues in information systems security: the insider threat,” *European Journal of Information Systems* (18:2), pp. 101–105.

Webster, J., and Watson, R. 2002. “Analyzing the past to prepare for the future: Writing a literature review,” *Management Information Systems Quarterly* (26:2).

Willison, R., and Backhouse, J. 2006. “Opportunities for computer crime: considering systems risk from a criminological perspective,” *European Journal of Information Systems* (15:4), pp. 403–414.

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

Wood, C. C. 2000. “An unappreciated reason why information security policies fail,” *Computer Fraud & Security* , pp. 13–14.

Yoo, C. W., and Lawrence Sanders, G. 2013. “An exploration of group information security compliance: A social network analysis perspective,” in *International Conference on Information Systems (ICIS 2013)*, , pp. 388–399.

Zack, M. 2000. “Researching organizational systems using social network analysis,” in *Proceedings of the 33rd Hawaii Conference on System Sciences*, (Vol. 00) , pp. 1–7.

Dang-Pham, Pittayachawan and Bruno © 2014. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.