2010

Understanding the Factors of Information Leakage through Online Social Networking to Safeguard Organizational Information

Nurul Nuha Abdul Molok
University of Melbourne, nurulnuha@iium.edu.my

Atif Ahmad
University of Melbourne, atif@unimelb.edu.au

Shanton Chang
University of Melbourne, shanton.chang@unimelb.edu.au

Understanding the Factors of Information Leakage through Online Social Networking to Safeguard Organizational Information

Nurul Nuha Abdul Molok
Department of Information Systems
University of Melbourne
Victoria, 3010
Email: n.abdulmolok@pgrad.unimelb.edu.au

Atif Ahmad
Department of Information Systems
University of Melbourne
Victoria, 3010
Email: atif@unimelb.edu.au

Shanton Chang
Department of Information Systems
University of Melbourne
Victoria, 3010
Email: shanton.chang@unimelb.edu.au

Abstract

With the rapid escalation of the online social networking (OSN) use, there have been some high profile cases reported in the media about information leakage by employees that are detrimental to organizations. However, academic literature rarely discusses the impacts of OSN on organizations. This conceptual paper explores employees' OSN use behaviour that leads to the disclosure of organizational information which may jeopardize the information systems (IS) security. In order to do that, the paper briefly reviews theories from criminology, psychology and sociology that are related to our study. We find that Decomposed Theory of Planned Behaviour is the most suitable theoretical model in explaining the underlying factors that drive information leakage through OSN. The understanding of these reasons facilitates our suggestion for organizations to safeguard information against this insider threat by employing information security education, training and awareness (SETA) programs for employees.

Keywords

Information leakage, unauthorised information disclosure, online social networking, information security

INTRODUCTION

An Israeli soldier leaked the location and time of an upcoming raid in his Facebook status update causing Israeli military to cancel the entire operation and expel him from his battalion (BBC 2010). Executives worry about employees using Facebook and Twitter since it leads to leakage of intellectual property and confidential information (Gaudin 2009) especially now that cybercriminals are targeting at online social networking (OSN) sites to steal proprietary information and storage (Westervelt 2009). The importance of securing organizational information from insider threats has been highlighted by industrial surveys which confirm that currently, employees around the world are putting corporate and personal information at risk through the use of OSN, thus increasing the challenge to protect sensitive information from leakage (CISCO 2008; Proofpoint 2009).

While information can be leaked through offline social networking such as meetings, conferences and publications (Jansen 2010) and other communication channels, the leakage through OSN is fundamentally different than its offline counterpart and other channels. It is because the moment employees post sensitive information on their sites, the published information is almost permanent, it can be reached by many people and, possibly be copied and distributed to someone else. If they leak information face-to-face to someone, possibly due to the slip of a tongue, the information is confined to the people who heard the conversation, and even if it is communicated to other people, it becomes hearsay.

The employees' careless behaviour in using OSN adds complexity to the problem. Research on Facebook shows that users are usually not careful about accepting friends' requests and using applications on the sites (Athanasopoulos et al. 2008; Gross and Acquisti 2005; Jagatic et al. 2007). Some users simply accept friends' requests to have higher number of friends within their social networks to indicate their popularity. They are not aware that the 'friend' that they add can be an external attacker who is conducting surveillance and collecting intelligence on their employer organizations. Similarly, these attackers can develop and upload applications that contain malware crawling inside users' computing platforms to steal information, sabotage the organization's network, or use organizational resources for launching attacks (Athanasopoulos et al. 2008). Furthermore, the rapid merging of systems and applications used at work and home is making it difficult for them "to have a true boundary between work and home life and that they spend time sharing personal and business information on social networking sites with a trusting innocence" (Colwill, 2010, p.4). As the result, employees often post business problems to seek advice from their contacts within their social networks disclosing sensitive information such as corporate IP addresses and other details about their computing platforms (Colwill 2010; McKenna 2009). Availability of mobile technologies and their compatibility to OSN applications further complicates this problem. It becomes more challenging for organizations to monitor OSN misuse as employees utilize personal mobile devices (Everett 2010; Young 2010), to constantly update what they are doing to everyone within their social networks from time to time (McKenna 2009).

OSN has become the global phenomenon nowadays, raising information security problems to the organizations due to its use among employees. Hence, we seek to explore the answers to these research questions: Why employees disclose organizational information on their OSN sites? How do organizations safeguard their information from being leaked by employees through OSN? With the understanding of the underlying factors that cause employees to disclose private information to the public domain, and the strategies utilized by organizations to address this problem, we offer our suggestion for organizations to address this problem in order to safeguard their information.

The paper starts with the importance of managing information security in organizations from insider threats. Next, it briefly covers the studies done in information leakage and subsequently exerts OSN as the most challenging driver of the threat. After that, we present a review of theories from multiple disciplines and posit the chosen theoretical model to explain this behaviour. Using the model, we provide the basis of employees' behaviour in leaking information via OSN. Finally, we offer the guideline for organizations to deal with the problem. This paper is conceptual and seeks to address the above research questions, pointing at the direction for further research.

INSIDER THREATS TO INFORMATION SECURITY

Despite reported information security cases and their impacts on organizations, information security research in information systems (IS) is still in its infancy (Zafar and Clark 2009). In fact, the definition of information security varies depending on one's stance, as Zafar & Clark (2009, p. 572) points out "it can be technical, behavioural, managerial, philosophical, and/or organizational". Following the international management systems standards for information security (ISO/IEC 2005), we define information security as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (ISO/IEC, 2005, p.viii). From this definition, we come to understand that in the current information age, the information security arena has expanded from a technical initiative to organizational concern (Ahmad et al. 2005; Ashenden 2008; Humphreys 2008).

Although protecting information has become an organizational concern, many organizations embrace digital technology to manage their information, thus neglecting the protection of information printed on paper and conversed by people (Ahmad et al. 2005; Herath and Rao 2009). Hence, Ahmad et al. (2005) propose the information-centric approach as oppose to computing- or technical-centric approach to securing information, as shown in Figure 1. The model informs information dynamically exist in the forms of physical, digital and cognitive media that must be appropriately managed and controlled by organizations. We concur with this information-centric approach that posits organizational protection strategies should focus on the information, regardless of where it resides, as improper control of the flow of information may lead to information leakage.

Based on academic research and industrial surveys, cases of fraud and abuse of organizational resources are caused by their employees, the insiders of organizations rather than outsiders (CISCO 2008; Colwill 2010; Theoharidou et al. 2005; Warkentin and Willison 2009; Workman and Gathegi 2007). However, many organizations focus more on controlling and monitoring external threats (Colwill 2010). Insider threats have the potential to cause more damage to organizations since they have legitimate and privileged access to facilities and resources, and the knowledge of the organization and its processes. Furthermore, research indicates that the security incidents caused by insiders happen to be more accidental than intentional (Colwill 2010; Loch et al. 1992; Vroom and von Solms 2004; Warkentin and Willison 2009) and accidental security incidents by insiders happen more often and could have greater potential for harm than malicious insider attacks (Colwill 2010).

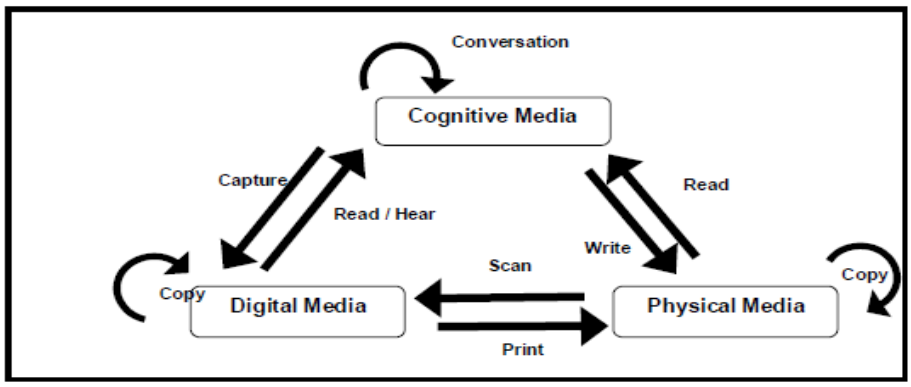

Figure 1: Information flow model (Ahmad et al. 2005)

The rise of OSN further complicates this issue since published information on the social media is instantaneously reached by wider audience from anywhere at any time, making it more challenging for organizations to control the flow of information. Colwill (2010, p. 3) points out that "there is an increase in the number of organizations damaged by sensitive information appearing on blogs and OSN sites". Not only that, OSN causes wasting of organizations' time and resources (Colwill 2010; Young 2010), putting organizations' networks and systems at risk of malware, leading to potential lawsuits due to copyright and defamation, and significantly impacting on organizational reputation and future revenue (Colwill, 2010). Hence, organizations need to find ways to address information leakage through the use of OSN to avoid these damages.

INFORMATION LEAKAGE AND ONLINE SOCIAL NETWORKING

Despite the interchangeable terms and definitions that describe information leakage, we define information leakage as "a breach of the confidentiality of information, typically originating from staff inside an organisation and usually resulting in internal information being disclosed into the public domain" (ISF 2007, p.2). Similar to other insider threats, many incidents of information leakage are accidental (ISF 2007). Information leakage or unauthorized disclosure of information is one of the threats to IS security (Loch et al. 1992) that needs to be addressed by organizations to safeguard their confidential and sensitive information. Literature informs that information can be leaked through:

- OSN or social networking sites (Athanasopoulos et al., 2008; Colwill, 2010; Gross & Acquisti, 2005; Leitch & Warren, 2009),
- conversation (Ahmad et al. 2005; Mitnick et al. 2002),
- email (Carvalho, Balasubramanyan, & Cohen, 2009),
- printing facilities (Ahmad et al. 2005; Mitnick et al. 2002)
- cloud computing (Ristenpart, Tromer, Shacham, & Savage, 2009),
- domain name systems (Rose, Chandramouli, & Nakassis, 2009),
- portable data devices (CISCO, 2008; Colwill, 2010), and
- offline social networking such as conference and publications (Jansen, 2010).

We view the most challenging channel of information leakage is OSN that comprises of social networking sites such as Facebook and LinkedIn (to name a few), blogs such as WordPress and Blogger, microblogging sites such as Twitter, contents (YouTube and Flickr), wikis (Wikipedia) and online forums (Mayfield 2008). OSN is unique from other platforms because it has some characteristics that make it easier for external attackers to do surveillance and gather intelligence, sabotage organizations' networks using malware and utilize resources to launch attacks through the applications embedded on OSN sites. These characteristics are the information posted on OSN almost permanent, instantaneous and accessible by anyone, at anytime, using any device. Moreover, employees' careless behaviour in accepting friends' requests, and constantly posting information and updating their status when they are at work or home, contributes to this 'uniqueness'.

Information disclosed in employees' sites can tarnish the reputation of an organization too. For example, through OSN, an employee may post information about the status of a confidential project or private meetings with stakeholders, or upload photographs or videos that cause embarrassment and libellous to the organization. It can be more difficult for organizations to address this problem due to the increasing use of personal mobile devices in accessing the social media. In Facebook alone, more than 150 million active users access the site via their mobile devices (Facebook 2010). Besides, it is difficult for organizations to control the flow of information through OSN, since posted information can be copied and distributed to other people outside their social networks in various forms (spoken in conversation, printed on paper or spread through emails). Therefore, we focus on OSN as it is the most challenging driver of information leakage compared to others.

Statistics show that the Internet activities globally are taking place on OSN. To date, OSN sites monopolizes the Global Top 10 Sites on the Web with Facebook at number two, followed by YouTube, Wikipedia, Blogger and Twitter (Alexa, 2010). According to Alexa (2010), Facebook is the most visited website in Indonesia, Malaysia, Phillipines and Singapore, and it is the second most visited website in U.S., U.K., Canada and Australia, to name a few. Currently there are more than 500 million Facebook active users and 50% of their active users access Facebook daily (Facebook 2010). OSN sites particularly Facebook, has become the global phenomenon nowadays, raising information security problems to the organizations and privacy issues to the individuals.

Although there are many studies done in OSN, the studies that discuss issues of information security in OSN are limited. If there are any, we found that most of them cover the implication of OSN to the individuals. Some of these studies are: information revelation in Facebook among university students (Gross and Acquisti 2005), the rise of privacy issues among teenagers since they are unaware about the nature of the Internet (Stutzman 2006) and OSN as the potential avenue for identity theft and malware attacks (Athanasopoulos et al. 2008; Jagatic et al. 2007). We acknowledge that studies about OSN impacts on individuals' privacy are important to both research and practice. However, it is beyond the scope of our study, as we concentrate on OSN security impacts on organizations.

So far, we have covered the insider threats to information security as an organizational concern, the importance for organizations to control and manage the information flow within various media and OSN as the most challenging channel of information leakage that is difficult for organizations to mitigate. Next, we will provide the review of theories related to this phenomenon and the reasons behind the employees' behaviour of leaking information through OSN informed by a theoretical model from IS.

THE REASONS BEHIND THE LEAK

This section is intended to answer the following question: Why employees disclose organizational information on their OSN sites? In order to answer this question, we explore theories from various disciplines used in IS studies to explain information security breaches by insiders. Subsequently, we posit the most suitable theory for this study to explain the factors that drive OSN users to disclose sensitive information that may have serious impacts on the organization.

Theoretical Background

One of the earlier studies on the development of theoretical models within OSN context uncovers the underlying human psychological factors that are driving the reasons why people engage in OSN, through the lens of Self Determination Theory (Sachdev 2007). In the study, it was found that factors that influence people to use OSN are: control (ability for users to change OSN sites' personalization options), responsiveness, reciprocal communication (between user-medium and user-user), social presence, self-representation and deep profiling (Sachdev 2007). The author claimed that this reformulation of interactivity construct is the first of its kind within the OSN context. Although OSN security issues were not captured in his study, he pointed out that control over users' access to information is vital since it has an impact to organizations. This calls for our contribution to fill in this gap, to explain why people engage in OSN behaviour that leads to disclosure of information that may affect the organizational information security, through the lens of a theoretical model.

With this aim, we explore several theories under organizational misbehaviour, organizational behaviour, criminology and social cognitive. Although information leakage can be considered as an organizational misbehaviour, we disregard the Model of Organizational Misbehaviour (Vardi and Wiener 1996) since it focuses more on intentional rather than accidental misbehaviour, where as employees' threats to IS security are often accidental than intentional. Under organizational behaviour, we find that Reinforcement Theory in the Workplace (Hamner, 1974 as cited in (Vandeveer and Menefee 2006)) is more suitable to explain employees' information security behaviour in organizations. According to the theory, "the consequences of an action (rewards and punishments) determine a person's motivation for engaging in certain behaviours" (Vandeveer & Menefee, 2006, p.54). Similarly, IS security studies show that this action contributes to information security compliance and the following describes some of the studies done in this area.

Some research in IS security use General Deterrence Theory (GDT), a criminology theory, to propose the use of information security policy, awareness training and preventive security systems as key deterrents to computer abuse (Straub 1990; Theoharidou et al. 2005; Workman and Gathegi 2007). In similar vein, some other IS security scholars use Prevention Motivation Theory (PMT), a social cognitive model, to explain why security breaches still happen although people are aware of IS security threats (Workman et al. 2008). Others combine PMT and GDT with the Theory of Reasoned Action (TRA) and IS success to propose a model that explains IS security compliance by employees (Pahnila et al. 2007) and combination of PMT-GDT with other theories such as Organizational Commitment and the Decomposed Theory of Planned Behavior to explore the intention to comply with information security policies (Herath and Rao 2009).

Theoharidou et al. (2005) further explore GDT and other criminology theories to investigate insider threats in IS security management focusing on information security standard described in ISO/IEC (2005). They found that GDT is significantly related to the standard compared to other theories. However, Pahnila et al. (2007) found that attitude, normative beliefs and habits have significant effects on the users' intention to comply with IS security policies compared to sanctions which is based on GDT. Another study supports this and proposes a theoretical model that explains non-compliance to IS security in terms of moral reasoning and values based on Theory of Cognitive Moral Development and Theory of Motivational Types of Values (Myyry et al. 2009). In contradiction, a study that investigates the relationship between attitudes toward the law, social influences, and self-control, found that punishment is effective in preventing information security threats (Workman and Gathegi 2007).

The studies described above explain about employees' behaviour in compliance to the information security policy of organizations, but the underlying factors about why they perform security incidents are still not clearly understood. Hence, concurring with the findings by Pahnila et al. (2007), we concentrate on attitude, normative beliefs and habits instead of punishment as a negative reinforcement to explain IS security behaviour. Below, we briefly explain about the Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM) and Decomposed Theory of Planned Behavior (DTPB) before stating our preferred theory to describe and explain the phenomenon under study.

Theory of Reasoned Action (TRA) is a social psychology theory that mentions behaviour intention is the driver of behaviour and intentions are formed by a person's attitude and subjective norm or social influence. Theory of Planned Behavior (TPB) is an extension of TRA with an additional construct called perceived behavioural control which means behaviour can happen even when people do not have a complete control over their behaviour (Ajzen 1991). This notion is important to our study since it exerts that people's behaviour can be accidental and intentional, and the behaviour is also caused by social influence and the person's attitude towards IS use. Research in IS shows that Technology Acceptance Model (TAM) is better than TRA and TPB to explain use intentions. TAM is an adaptation of TRA which specifies two beliefs; perceived usefulness and perceived ease of use, as the determinants of attitude that results to intentions and IT use (Davis, 1989 as cited in (Taylor and Todd 1995)). However, according to Taylor & Todd (1995), what influence the person to perform the behaviour is better explained by decomposing the attitudinal, normative and control belief structures. Hence, they proposed Decomposed Theory of Planned Behavior (DTPB) by combining TAM with TPB. We concur with Herath & Rao (2009) that DTPB provides a more complete understanding of behaviour within the IS context since it "explores multiple dimensions of subjective norms, and decomposes the perceived behavioural control dimension to evaluate self-efficacy along with technology and resource facilitating conditions" (Herath & Rao, 2009, p. 108). Figure 2 shows the DTPB model.

Therefore, we conclude that DTPB is the most suitable model to answer this question: Why employees disclose organizational information on their OSN sites? Furthermore, the model is also closely related to Sachdev (2007)'s findings on why people use OSN as described above, plus, DTPB explains that behaviour can happen intentionally and accidentally, in line with IS security findings that show insider threats to organizational information security are mostly due to accidental behaviour. Below we explain why an employee discloses organizational sensitive information through the use of OSN using DTPB model.

Decomposed Theory of Planned Behavior

The attitude construct of the model portrays that positive attitude towards IS use is based on perceived advantages (usefulness), simplicity (ease of use) and compatibility of the use to needs and values (Taylor & Tood, 1995). OSN sites such as Facebook is designed to be easy to share and exchange information. In fact, its ease of use is key to their popularity (Everett 2010). OSN is also perceived both useful for individuals, being in contact with their family and friends in their social networks, and for organizations, using OSN as free marketing strategies and increase reach to customers. Focusing on the individuals, the ease of using OSN, allows users to connect to one user to another to increase their social networks. Despite the usefulness, it has its downside to information security. Since it is easy for OSN users to search for a friend using the search function provided by the OSN site, it is as easy for a cybercriminal to find his/her victims. For example, a cybercriminal who is hired by an organization to do industrial espionage against another organization will seek for OSN users who are the employees of the victim organization. The cybercriminal then sends them friends' requests and once the requests are accepted, he/she can collect as many information as possible to realize the attack. Similarly, since it is easy to launch applications on OSN sites like Facebook, cybercriminals can create applications that can crawl into employees' profiles to search and collect potential information or even install malware through the application to launch attacks (see Athanasopolous et al., 2008 and Jagatic et al., 2007 for details). The third determinant of attitude towards IS use is compatibility, which means the degree to which the IS fits the users' existing values, previous experiences and current needs (Taylor and Todd 1995). For example, employees may think that by using

their own computing devices, it is not wrong to access to their OSN sites within working hours. They do not realize that they actually cause financial losses due to the decrease in the organization's productivity.

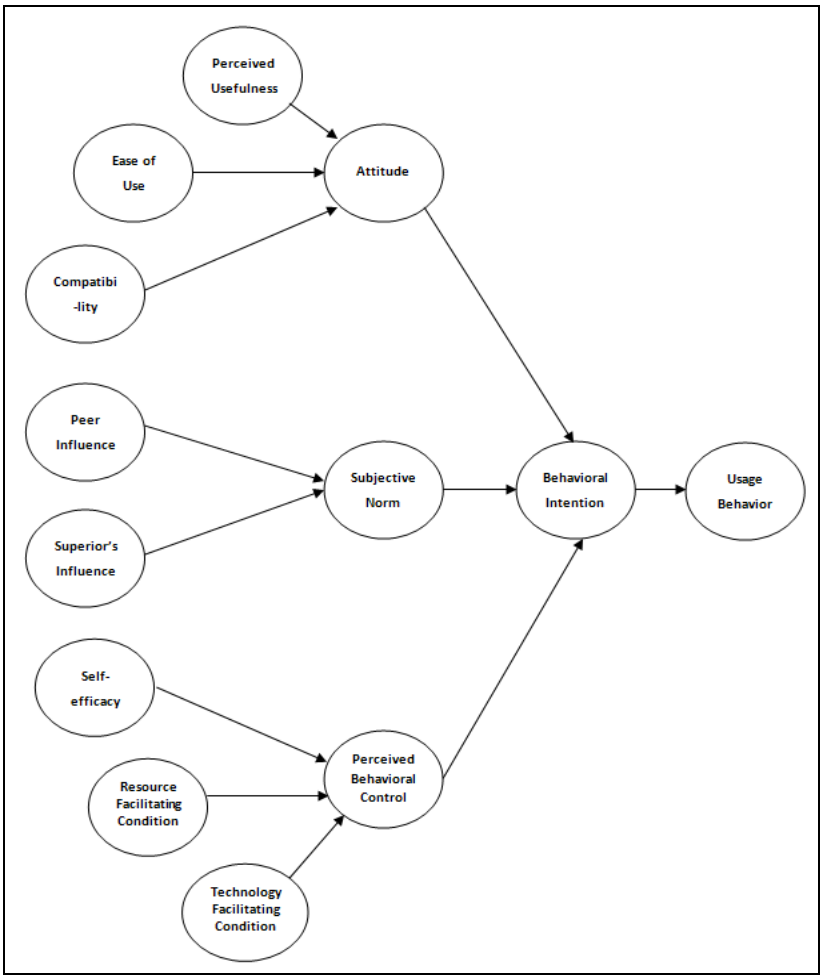

Figure 2: Decomposed theory of planned behaviour (Taylor & Todd, 1995)

In subjective norms, peer influence and superior's influence also play a role to determine the intention to perform the behaviour. Other employees and the organization can influence an employee to engage in OSN to reveal information. For example, knowing there are contacts in employees' social networks who can help them with a problem in system administration tasks (peer influence), and there is no policy about keeping confidential information from being disclosed through OSN in the organization (superior influence), employees post the details of the system problem on their LinkedIn site. They do not realize that they are posting confidential information that is stored and searchable in the public domain which put the organization in the danger of a cybercriminal's attack. In this scenario, we can say that their behaviour is intentional in a non-malicious way but their ignorance and negligence about information security puts the organization in jeopardy. Sometimes employees cut security corners for their own convenience too. They know revealing corporate systems information is wrong but the demand of work productivity or pressure from their boss to solve the problem fast, made them do it anyway.

Perceived behavioural control that drives the intention to perform behaviour within IS context is the main reason why we chose DTPB as the preferred model to explain OSN users' behaviour that lead to information leakage. While other theories mostly explain about behaviour that is intentional, DTPB exerts that behaviour can be accidental and intentional since it is performed within and beyond the person's control. Determined by self-efficacy (perceived ability) and facilitating conditions in terms of resources and technology, OSN users perform behaviours that are both accidental and intentional. For example, employees may use the computing facilities provided by the organization to access OSN sites, but if the organization restrict the use of OSN within working hours, the employees can still use their personal mobile devices as an alternative. Mobile devices facilitate the OSN use behaviour that allow users to constantly update what they are doing and express their feelings from time to time, thus, revealing unintended work-related information to the public domain that might be sensitive to the organization.

The examples for every constructs in the DTPB model given above are not limited to other OSN behaviours that violate organizational information security. Table 1 shows the summarized explanation of the examples including other cases about employees' OSN behaviour and the implications to organizations based on DTPB.

This section provides the explanation of why employees use OSN to perform behaviour that leads to the organizational information security problems especially due to the leakage of information to the public domain. The next section proposes the guideline for organizations to address this behaviour.

Table 1. Factors of Information Leakage through OSN based on DTPB

DTPB Construct	OSN use behaviour	Implication to organization
Attitude towards the use of OSN (Perceived ease of use, Perceived usefulness, Compatibility)	Carelessness in posting information, sharing photo and videos, accepting friends' requests, clicking on external links and using third party applications	Employees become the target of cyber criminals Decrease organization's productivity
Subjective norms (Peers' influence, Superior's influence)	Since everyone is doing it, it is OK (blurring work ethics) Demand for work productivity No OSN guidelines specified in the information security policy	Post sensitive information to solve work-related problems Expose information to cybercriminals
Perceived behavioural control (Self-efficacy, Resources and Technology facilitating conditions)	Accidental and non-malicious disclosure of information Accidental and malicious disclosure of information (posting sensitive information and inappropriate photos and videos through mobile devices) Intentional and non-malicious disclosure of information (popularity, showing off, convenience) Intentional and malicious disclosure of information (disgruntled employee, espionage, sabotage)	Decrease organization's productivity Tarnish reputation of organization Financial damage to organization

PREVENTION OF INFORMATION LEAKAGE THROUGH OSN

Since information leakage through OSN cause damages to organizations, it is essential for organizations to address employees' behaviour that lead to this predicament. This section provides the safeguarding measures for organizations to address this problem and answers the following question: How do organizations safeguard their information from being leaked by employees through OSN?

IS security literature proposed information security policy, awareness training and preventive security systems as key deterrents to insider's threats (Straub 1990; Theoharidou et al. 2005; Workman and Gathegi 2007). However, which one of these measures is the most suitable to avoid information leakage through OSN by employees? Say an organization has a security policy to limit the use of OSN during working hours, and to implement this, it utilizes a preventive security systems to automatically restrict access to OSN. These methods may be capable to prevent access to OSN using the organization's computing devices, but employees can still connect to OSN using their personal mobile devices and home PCs. In this case, sensitive organizational information can still be leaked, making security policy and preventive systems ineffective to prevent information leakage through this channel. Hence, we propose the implementation of information security education, training and awareness (SETA), as the approach to mitigate this problem. SETA program is able to improve employees' behaviour, and enable organizations to hold employees accountable for their actions (Whitman and Mattord 2008). Furthermore, it is able to increase employees' perceptions of vulnerability and severity of information security threats although they do not experience any security incidents (Workman and Gathegi 2007).

According to Whitman and Mattord (2008), the rationale behind a SETA program which encompasses these elements; security education, security training and security awareness, is to improve organizational information security by:

- building in-depth knowledge to design, implement, or operate security programs for organizations and systems through **security education** for employees with information security responsibilities,
- developing employees' skills to perform their jobs while using IS more securely through **security training**, and

- improving employees' awareness to protect IS resources through **security awareness** programs.

Table 2 shows the difference of these elements in SETA program in terms of their attribute, level, objective, method, test measure and impact timeframe.

Table 2. Difference of Elements in SETA framework (Whitman and Mattord 2008)

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media • Videos • Newsletters • Posters, etc	Practical Instruction • Lecture • Case study workshop • Hands-on practice	Theoretical Instruction • Discussion seminar • Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Previously, we mentioned the underlying factors that drive employees' behaviour are the determinants of the behavioural intention explained by DTPB model. These factors are; the attitude of employees towards OSN use, social influence from peers and superiors and perceived behavioural control that is determined by self-efficacy and facilitating conditions. Below we show how SETA can tackle this issue by addressing these factors.

As stated earlier, the attitude towards OSN use behaviour is based on the perceived ease of use and usefulness, and compatibility. As McKenna (2009, p. 19) pointed out "The problem is that it is so easy. Social networking sites ask you 'what are you doing now?' and you respond". SETA programs should alert employees about the ease of OSN use may result to the difficulty of controlling sensitive information appearing on OSN sites. Once an employee posts information, it is almost impossible to control the flow of information because it is as easy for anyone to copy and distribute the information to other people.

With regard to subjective norms or social influence, organizations need to make it mandatory for all employees regardless of levels and positions to attend the awareness training sessions on the acceptable use of OSN and its impacts on information security. An organization wide SETA is vital to ensure employees understand their information security responsibilities, organizational policies and proper use of IT resources entrusted to them (NIST 2003). Besides, their superiors' attendance may indicate the organization's seriousness about irresponsible use of OSN and its expectation to each staff. This may influence them to be more aware about proper use of OSN and be more responsible when they are using the social IS in the future.

The final and most important factor, perceived behavioural control, shows that employees leak information through OSN, whether accidentally or intentionally, that may cause great impacts on organizations. Similar to other insider threats, this problem is perceived to be more accidental than intentional especially due to pervasive use of mobile devices to access OSN sites. SETA is deemed to be capable to minimize accidental security breaches (Whitman and Mattord 2008). Therefore, organizations should provide security education for staff with information security responsibilities to design security awareness programs that inform all employees about careless use of OSN could lead to damages to the organization. The awareness will result to more mindful use of OSN behaviour particularly in accepting friends' request and using applications on the sites. It is also imperative for the organization to clearly state the repercussions of this problem to the organization as well as to the employees. Once the organization's reputation is damaged, they will lose customers' trust and loyalty, thus financial instability may occur which can cause the employees to lose their jobs. This understanding will definitely prevent accidental leakage of information through OSN.

In this section, we propose that SETA program is able to prevent information leakage through OSN by addressing the underlying factors that influence this behaviour. The approach to understand human behaviour in order to address the behaviour that leads to security problems is an area worth researching since it defies traditional convention of information security solutions through technical approach. Although we acknowledge that information security policy and preventive security systems are also able to address this problem, we suggest that more research in this area is required focusing on behavioural facets of information security, in order to verify the claim that SETA is the better approach to minimize this problem.

CONCLUSION

Organizations face more challenges in protecting their information due to employees' careless behaviour while using OSN that leads to unintended leakage of confidential and sensitive information. The paper has examined why employees leak information through OSN and how organizations should deal with it to safeguard their information. The flow of information published on OSN sites is difficult to control since it can be stored in various formats, copied and distributed to other people. This creates an avenue for external attackers to carry out surveillance and gather intelligence to launch attacks, thus making OSN as the significant vehicle of information leakage. Furthermore, it is accessible by anyone, using any devices at any time, causing sensitive information leakage capable of tarnishing the organization's reputation.

To prevent this problem, we explored the underlying factors of employees' behaviour in leaking information through the use of OSN. In order to do that, we reviewed theories from criminology, psychology and sociology disciplines to help us explain this behaviour and found that Decomposed Theory of Planned Behavior (DTPB) is the most suitable theoretical model for this study. Its attitude, subjective norm and perceived behavioural control (PBC) constructs are able to describe and explain this behaviour. We also found that PBC is the best predictor since it demonstrates OSN use behaviour that leads to information leakage can be both accidental and intentional. Employees often unthinkingly post information, not realizing that the information is stored and searchable by other people. Therefore, we proposed that organizations should design and implement information security education, training and awareness (SETA) programs for all employees to address this problem while stressing the need for further research in this area.

This study offers contributions to the IS security research and practice. It addresses the research gaps concerning the behavioural facets of information security and OSN security impacts on organizations. It is also perceived as timely and important considering the current media attention to this phenomenon.

REFERENCES

Ahmad, A., Ruighaver, A.B., and Teo, W.T. 2005. "An Information-Centric Approach to Data Security in Organizations," *TENCON 2005 2005 IEEE Region 10*, pp. 1-5.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Process* (50:2), December, pp 179-211.

Ashenden, D. 2008. "Information Security Management: A Human Challenge?," *Information Security Technical Report* (13:4), pp 195-201.

Athanasopoulos, E., Makridakis, A., Antonatos, S., Ioannidis, S., Anagnostakis, K., and Markatos, E. 2008. "Antisocial Networks: Turning a Social Network into a Botnet," *11th Information Security Conference (ISC 2008)*, Taipei, Taiwan.

BBC. 2010. "Israeli Military 'Unfriends' Soldier after Facebook Leak." Retrieved 9 March 2010, from http://news.bbc.co.uk/2/hi/middle_east/8549099.stm

CISCO. 2008. "Data Leakage Worldwide: Common Risks and Mistakes Employees Make," in: *CISCO Systems White Paper*. San Jose, CA: CISCO Systems Inc.

Colwill, C. 2010. "Human Factors in Information Security: The Insider Threat - Who Can You Trust These Days?," *Information Security Technical Report* (in press).

Everett, C. 2010. "Social Media: Opportunity or Risk?," in: *Computer Fraud & Security*. pp. 8-10.

Facebook. 2010. "Facebook Statistics." Retrieved 14 Sept 2010, from http://www.facebook.com/press/info.php?statistics

Gaudin, S. 2009. "Execs Worry That Facebook, Twitter Use Could Lead to Data Leaks." *ComputerWorld* Retrieved 2 June 2010, from http://www.computerworld.com/s/article/9136465/Execs_worry_that_Facebook_Twitter_use_could_lead_to_data_leaks

Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks (the Facebook Case)," *ACM Workshop on Privacy in the Electronic Society (WPES), 2005*, Virginia, USA: ACM.

Herath, T., and Rao, H. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18), pp 106-125.

Humphreys, E. 2008. "Information Security Management Standards: Compliance, Governance and Risk Management," *Information Security Technical Report* (13:4), pp 247-255.

ISF. 2007. "Information Leakage." *Information Security Forum Briefing No.4* Retrieved 19 November 2009, from www.securityforum.org

ISO/IEC. 2005. "Information Technology - Security Techniques - Code of Practice for Information Security Management," in: *ISO/IEC 17799:2005(E)*. Geneva, Switzerland: ISO/IEC.

Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F. 2007. "Social Phishing," *Communications of the ACM* (20:10), pp 94-100.

Jansen, J. 2010. "Strategic Information Disclosure and Competition for an Omperfictly Protected Innovation," *The Journal of Industrial Economics* (58:2), pp 349-372.

Loch, K.D., Carr, H.H., and Warkentin, M.E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp 173-186.

Mayfield, A. 2008. "What Is Social Media?." iCrossing e-book.

McKenna, B. 2009. "Awareness Training 2.0," in: *InfoSecurity*. pp. 18-21.

Mitnick, K., Simon, W., and Wozniak, S. 2002. *The Art of Deception: Controlling the Human Element of Security*. New York: John Wiley & Sons.

Myyry, L., Siponen, M., Pahnila, S., Vartiaine, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18), pp 126-139.

NIST. 2003. "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology, Maryland, U.S.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *40th International Conference on System Sciences*, Hawaii: IEEE Computer Society.

Proofpoint. 2009. "Outbound Email and Data Loss Prevention in Today's Enterprise," California.

Sachdev, V. 2007. "Why Do People Engage in Social Computing? A Need Fulfillment Perspective," in: *Information Systems & Operations Management*. Texas, U.S.: The University of Texas at Arlington, p. 112.

Straub, D. 1990. "Effective Is Security," *Information Systems Research* (1:3), pp 255-276.

Stutzman, F. 2006. "An Evaluation of Identity Sharing Behavior in Social Network Communities," *International Digital Media and Arts Association* (3:1), pp 10-18.

Taylor, S., and Todd, P. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research* (6:2), June, pp 144-176.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The Insider Threat to Information Systems and the Effectiveness of Iso17799," *Computers & Society* (24), pp 472-484.

Vandeveer, R.C., and Menefee, M.L. 2006. *Human & Behavior in Organizations*. Upper Sadle River, New Jersey: Pearson Education, Inc.

Vardi, Y., and Wiener, Y. 1996. "Misbehavior in Organizations: A Motivational Framework," *Organization Science* (7:2), pp 151-165.

Vroom, C., and von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers & Security* (23), pp 191-198.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18), pp 101-105.

Westervelt, R. 2009. "Botnet Masters Turn to Google, Social Networks to Avoid Detection." Retrieved 28 January 2010, from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1373974,00.html

Whitman, M.E., and Mattord, H.J. 2008. *Principles of Information Security*. Stamford, Connecticut: Course Technology.

Workman, M., Bommer, W., and Straub, D. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24), pp 2799-2816.

Workman, M., and Gathegi, J. 2007. "Punishment and Ethics Deterrents: A Study of Insider Security Contravention," *Journal of the American Society for Information Science and Technology* (58:2), pp 212-222.

Young, K. 2010. "Policies and Procedures to Manage Employee Internet Abuse," *Computers in Human Behavior* (26), pp 1467-1471.

Zafar, H., and Clark, J.G. 2009. "Current State of the Information Security Research in Is," *Communications of the Association for Information Systems* (24:34), pp 572-596.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their helpful comments. Nurul Nuha Abdul Molok's PhD research is financed by the Malaysian Ministry of Higher Education and International Islamic University Malaysia.

COPYRIGHT