PACIS 2011 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

9 July 2011

Exploring The Use Of Online Social Networking By Employees: Looking At The Potential For Information Leakage

Nurul Nuha Abdul Molok
The University of Melbourne, n.abdulmolok@student.unimelb.edu.au

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

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

ISBN: [978-1-86435-644-1]; Doctoral consortium paper

EXPLORING THE USE OF ONLINE SOCIAL NETWORKING BY EMPLOYEES: LOOKING AT THE POTENTIAL FOR INFORMATION LEAKAGE

Nurul Nuha Abdul Molok, Department of Information Systems, The University of Melbourne, n.abdulmolok@student.unimelb.edu.au

Atif Ahmad, Department of Information Systems, The University of Melbourne, atif@unimelb.edu.au

Shanton Chang, Department of Information Systems, The University of Melbourne, shanton.chang@unimelb.edu.au

Abstract

The proliferation of online social networking (OSN) in recent years has caused organizations information security threats due to disclosure of information by their employees on their sites. The accessibility of OSN to anyone, at any time, using any devices, causes confidential and sensitive organizational information to be disclosed to unauthorised individuals, whether accidentally or intentionally. This study aims to explore this current phenomenon by investigating OSN use behaviour among employees that leads to information leakage through the lens of Decomposed Theory of Planned Behavior. It also seeks to investigate the strategies utilized by organizations to control such use and propose a control framework that effectively safeguards organizational information security from this threat.

Keywords: Information leakage, unauthorized disclosure, online social networking, social media, information security management.

1 INTRODUCTION

Information can be leaked via many means of communication channels but the rise of online social networking (OSN) makes it more challenging for organizations to prevent their valuable information from being disclosed to unauthorized parties. OSN sites or social media in this context involve social networking sites (Facebook, LinkedIn and MySpace), microblogging (Twitter), content communities (YouTube and Flickr), blogs and wikis (Mayfield, 2008). Often times, the media and surveys from the information technology industry report about cases of information breach, loss and leakage through OSN that cause damage to organizations' reputation and financial resources (Gaudin, 2009; Goodchild, 2010; Sophos, 2010; Verizon & USSS, 2010). Nevertheless, the academic literature seldom discusses the information security impacts of OSN on organizations as research on OSN typically focused on privacy issues, self presentation, network analysis and social capital benefits (DiMicco et al., 2008). Thus, the current phenomenon of information leakage through OSN and its impacts on organizational information security captured our interest to investigate this problem.

Literature informs that information leakage through OSN have caused detrimental impacts on organizations in terms of loss of productivity, 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; Gudaitis, 2010; Young, 2010). Realizing this, the study aims to explore and explain the use of OSN sites by employees that can jeopardize the confidentiality of organizational information, to investigate the strategies implemented by organizations in dealing with this problem, and subsequently propose a control framework that can be used to address this issue.

OSN is accessible anytime, anywhere, using any devices causing employees to update their status to their social networks several times a day. By doing so, they can inadvertently reveal sensitive information to the public about attending private meetings, going on a business trip, seeking advice to solve work problems and the list goes on. Employees' accidental and careless behaviour while using social media adds more complication to the phenomenon. If employees are not careful about accepting friends' requests, they could add 'enemies' instead of 'friends' who would have more access to their information (Goodchild, 2010). Additionally, they may click on links sent by seemingly legitimate 'friends' or use applications on OSN sites making them vulnerable to malware infection (Everett, 2010). These malware may contain a Trojan or backdoor connected to a remote command-and-control server that collects intellectual property and sensitive information of the targeted information through its employees (Athanasopoulos et al., 2008; Smith & Toppel, 2009).

The study employs Decomposed Theory of Planned Behavior (DTPB) (Taylor & Todd, 1995) as the underlying theory for the research design in guiding the development of interview questions and framing the data analysis. DPTB is chosen because it provides the means to describe and explain the social IS use among employees that contribute to the leakage of private organizational information to the public domain.

2 RESEARCH QUESTIONS

To achieve the aims of this study, below are the research questions that this study seeks to answer:

Research Question 1: Why do employees disclose sensitive organizational information on their OSN sites?

This question attempts to discover, describe and explain employees' OSN use behaviour such as posting personal and work-related information on their OSN sites, their response to friends' requests and comments, the use of OSN applications (i.e. games, photo and video sharing) and other activities. The understanding of employees' OSN behaviour that may contribute to information leakage will be used to support the recommendation of solutions for organizations to address this issue.

Research Question 2: How do organizations safeguard their information from being leaked by employees through OSN? Why do they utilize these safeguarding measures?

In OSN, the patterns of disclosure are unique, the impact of disclosure can be high and it is susceptible to other threats like identity theft, malware and social engineering. Therefore, this study will investigate how organizations deal with their employees using OSN; either by using information security policy, security education, training and awareness (SETA), and/or employing preventive security systems, and the reasons for employing these strategies. The answers to this question will provide the current scenario of organizations under study in terms of their security maturity practices in addressing this issue. Similar to the above question, the understanding of organizational strategies to combat information leakage will be used to recommend control mechanisms to prevent this problem.

3 KEY BACKGROUND LITERATURE

This study defines 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). It is one of the insider threats to information systems that needs to be controlled by organizations to ensure their confidential information is secured and protected. This threat can be caused by human and non-human perpetrators from inside or outside the organization (Loch, Carr, & Warkentin, 1992) through many different channels such as OSN (Gross & Acquisti, 2005), face-to-face conversation and printing facilities (Ahmad, Ruighaver, & Teo, 2005), email (Carvalho, Balasubramanyan, & Cohen, 2009), cloud computing (Ristenpart, Tromer, Shacham, & Savage, 2009), domain name systems (Rose, Chandramouli, & Nakassis, 2009) and portable data devices (CISCO, 2008).

Among these channels, we view OSN as the most challenging channel of information leakage since the leaked information will assist external attackers to do surveillance and gather intelligence, sabotage organizations' networks using malware and utilize resources to launch attacks through the applications on OSN sites (Gudaitis, 2010; Smith & Toppel, 2009). Moreover, through OSN sites, employees may post inappropriate information, photographs and videos that could cause embarrassment to the organizations. In fact, industrial surveys report that 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). It is important to note that, prior to the reported cases of information leakage via OSN involving high profile individuals throughout 2009, organizations were concern about their employees engaging in OSN because it wasted organizations' time and drain the bandwidth, but now, although productivity is still the concern, organizations are more worried about their confidential information being leaked via OSN (Gaudin, 2009; Sophos, 2010)

The rapid merging of systems and applications used at work, home and while on-the-go adds complications to this problem, thus, making it difficult for employees "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, thus disclosing sensitive information such as corporate IP addresses and other details about their computing platforms to the public domain (Colwill, 2010; McKenna, 2009). Furthermore, the 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).

Studies on Facebook shows that users tend to disclose too much information about themselves even though they do have some privacy expectations (Christofides, Muise, & Desmarais, 2009; Gross & Acquisti, 2005; Stutzman, 2006). Based on the studies, the types of information that users disclosed are full names, birthdates, address, phone numbers, education information, photos of themselves and others. Although the authors show that these types of information have implications on individuals' privacy, implications on organizations are not discussed. Similarly, a more recent study shows these personal information are being posted on users' profiles but the authors also include work information that describe users' employers' name, their position in past and present workplace(s), work description and time period (Nosko, Wood, & Molema, 2010). Despite the focus on the implications of information disclosure on individuals and the absence of coverage on organizational information security impacts, it is imperative to note that work information is also being published on OSN which indicates potential implications on organizations.

In terms of preventing information leakage, IS security literature proposed information security policy, awareness training and preventive security systems as key deterrents to insider's threats (Straub, 1990; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Workman & Gathegi, 2007). The question is, which one of these provides the most effective preventive measure to control this problem? As the outcome of this study, the control framework deemed to be the most effective mechanism for organizations to safeguard their information from leakage will be proposed.

4 THEORETICAL FOUNDATIONS

The study started with identifying several related theories in Information Systems (IS), psychology and criminology to provide the lens to further understand why security breaches occur and how employees contribute to IS security violations. With the understanding of the nature and application of the identified theories, we found that these theories mainly explain about employees' behaviour in compliance to the information security policy of organizations. Since we want to discover the underlying factors about why people perform security incidents, we concentrate on attitude, normative beliefs and habits to explain IS security behaviour. We find that Taylor-Todd's Decomposed Theory of Planned Behavior (DTPB) is the most suitable theoretical model for this study. Therefore, we concur with Herath & Rao (2009, p.108) 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). Based on DTPB, IS use is determined by the intention to perform the behaviour and the behaviour intention is driven by these three factors: attitude, subjective norms or social influence and perceived behavioural control (Taylor & Todd, 1995). Below, the application of DTPB in information leakage through OSN is given based on the conceptual findings from the academic literature, industrial surveys and the media.

The attitude construct of the model portrays that positive attitude towards IS use is determined by perceived advantages (usefulness), simplicity (ease of use) and compatibility of the use to their values, experience and needs (Taylor & Todd, 1995). Both individuals and organizations use OSN because it is perceived as a useful tool to them. Individuals use OSN to maintain close relationship with their social networks and to share thoughts, interests and events. Organizations use OSN as free marketing strategies and to increase reach to customers. In terms of simplicity, 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) since anyone, regardless of age and gender, are using OSN adding to 500 million users of Facebook in July 2010 (Facebook, 2010). Since many users are frequently available on their OSN sites, OSN becomes the platform for employees to solve work-related problems by seeking advice from their friends (Colwill, 2010; McKenna, 2009), which is an example to describe users' engagement in OSN because it is compatible to their needs. Despite its usefulness, it has a major downside to security. It is also easy for cybercriminals to launch targeted attacks on victim organizations. They can effortlessly find key employees of the organization, use a social engineering method to befriend them to bypass privacy settings imposed on their profiles, collect information about their organizations and employees' credentials, and invite the employees to use an application that actually installs Trojans or backdoors to gain greater access into the organization's networks.

The second construct is social influence from peers and superior which play a great role on users' participation in OSN. OSN is considered as the in-thing today that not participating in it may be considered outdated. Being influenced by peers engaging in OSN not only blurs the work ethics but it also contributes to financial losses. The absence of security guidelines on the use of OSN in organizations (superior's influence) makes employees unaware that they are contributing to the loss of productivity, strains on corporate bandwidth, damage to organizations' reputation, and more serious damage; cybercriminal's sabotage and espionage on the organizations.

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. Similar to other insider threats, information leakage through OSN is perceived to be more accidental than intentional especially due to the pervasive use of mobile devices. Based on the third construct, perceived behavioural control, the intention to perform IS use behaviour is determined by self-efficacy (perceived ability) and facilitating conditions in terms of resources and technology. An accidental information leakage via OSN can happen when employees are using their personal devices such as their ubiquitous smartphones. The ‘always on’ environment allows employees to constantly update their status and, upload photos and videos on their OSN sites, thus inadvertently releasing private work-related information to the public domain. This posted information not only tarnishes organizations’ reputation, but it can be gathered and deduced by attackers to conduct espionage on organizational confidential and sensitive information.

On the other hand, information leakage through OSN can be done intentionally with and without malicious intent. For example of an act of malicious intent, a disgruntled employee may disclose libellous information about the organization on OSN sites, as reported in a study by Verizon and US Secret Service that a terminated system administrator stole a co-worker’s password for his OSN site and modified it with slanderous content (Verizon & USSS, 2010). As an example to intentional information leakage without malicious intent, an employee may deliberately expose the news about the merging of companies before it is formally made public out of enthusiasm.

In this section, we have seen how and why employees use OSN based on the determinants of IS use behaviour from DTPB model based on the literature, literally answering the first research question. Based on this model, information leakage through OSN is driven by: a) the users’ attitude due to its simplicity and perceived usefulness, b) social influence from peers and superior, and c) perceived behavioural control which explains that while using the IS, the behaviour can be accidental and intentional, due to users’ perceived ability, available resources and technologies that facilitate the behaviour. The understanding of these underlying factors will be used to assist the design of interview questions, data analysis and recommendation of solutions for this problem.

4.1 Conceptual Model of Information Leakage through OSN

Figure 1 shows the conceptual model of this study applied from the DTPB theoretical model, which depicts that information leakage can occur through the use of OSN among employees due to the underlying factors determined by the theoretical model. The conceptual model depicts OSN use behaviour which is derived from the literature and the relationship with the determinants from DTPB model. It shows that behavioural intention which leads to OSN use is due to the user’s attitude, social influences and control factors in the organization that influence the use. The use of OSN can contribute to leakage of information to the public domain that affects the information security of an organization. We propose that the leakage can be addressed by a control framework which consists of security policy, security education, training and awareness (SETA) program and preventive systems that is able to control the factors of OSN use behaviour among employees.

Upon completion of this research, the actual reasons of employees exposing confidential organizational information through the use of OSN and the strategies utilized by organizations to prevent it will materialize. The reasons are expected to revolve around the factors determined by DTPB model and the OSN use behaviour may be extended to more OSN functionalities that can contribute to leakage. The expected effective prevention method is the combination of security policy, SETA and preventive systems or other forms of control mechanisms.

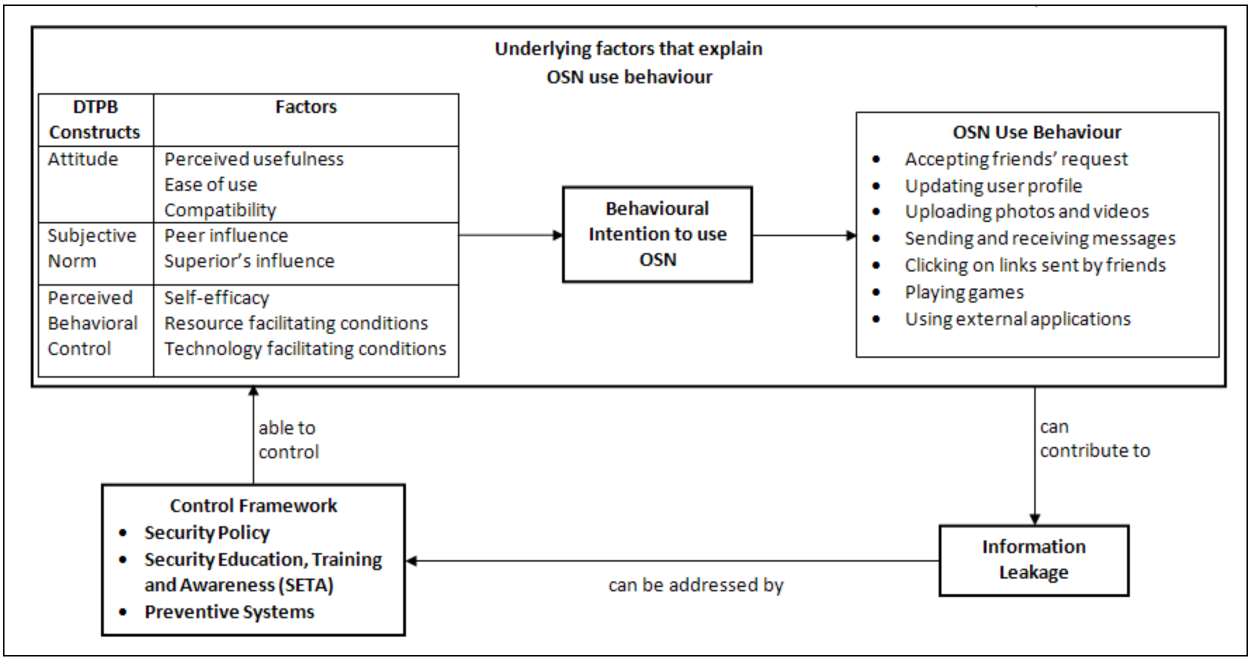
Underlying factors that explain OSN use behaviour
DTPB Constructs
Factors
Attitude
Perceived usefulness
Ease of use
Compatibility
Subjective Norm
Peer influence
Superior's influence
Perceived Behavioral Control
Self-efficacy
Resource facilitating conditions
Technology facilitating conditions
Behavioural Intention to use OSN
OSN Use Behaviour
Accepting friends' request
Updating user profile
Uploading photos and videos
Sending and receiving messages
Clicking on links sent by friends
Playing games
Using external applications
able to control
can contribute to
Control Framework
Security Policy
Security Education, Training and Awareness (SETA)
Preventive Systems
can be addressed by
Information Leakage

Figure 1. The Conceptual Model

5 PROPOSED METHODOLOGY

The research questions require the researcher to describe the phenomenon of information security in the organizations as well as to understand human actors and their OSN use behaviour in their social settings. Based on the research questions specified earlier, the research design that is proposed for this study is depicted in Figure 2.

Based on Figure 2, the study is divided into four phases. Phase 1: Contextual Study comprises the definition of research context and review of literature on topics relevant to this study.

Phase 2 is the empirical investigation to answer the first research question. This phase involves multiple case studies on four organizations to investigate the employees' OSN use behaviour that contributes to leakage of information. The organizations are chosen due to the use critical information in their operations. These organizations are all based in Malaysia and they are:

- a tertiary education provider for local and international students
- a security services provider
- an agency responsible for managing information and communication technologies
- an organization responsible for regulating for the communication and multimedia industry

Data has been collected by interviewing 22 employees who are the users of OSN and observing their activities on these sites. In this phase, the OSN activities under investigation are their wall updates, their response to friends' requests and comments, the use of applications such as games, photo and video sharing, the types of information disclosed (personal and work-related information), and to whom it is disclosed to whether accidentally or intentionally (for e.g. the information is intended for friends only but ended up being disclosed to everyone). Data analysis of the output will be carried out and the results will support the design of interview questions in the next phase. As mentioned earlier, DTPB model will be used to guide the design of interview questions and data analysis.

Phase 3 involves empirical investigation to answer the second research question to investigate organizational strategies to control information leakage via OSN. The four cases above will be revisited but this time data will be collected by interviewing the people in the management level who are involved in the information security management, such as Chief Information Security Officer

(CISO), IT manager and HR manager. This will be followed by observations and documents (for e.g. information security policy and training manual) review. Data analysis of the output will then be carried out and the results will assist the recommendation of the most effective control mechanism to address this issue in the final phase.

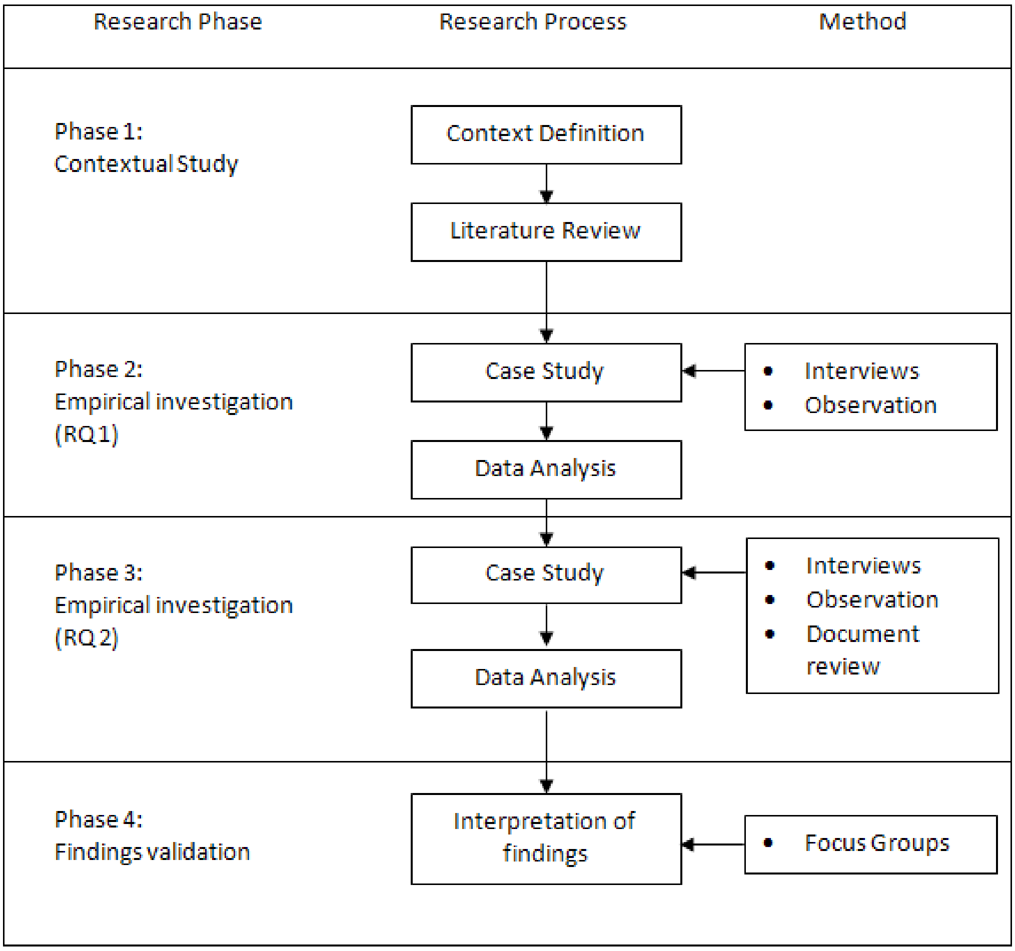

Figure 2. The Research Design

At Phase 4, it is expected that all research questions will be answered by analysing and reflecting on the collected data which is guided by the literature. The findings are validated through comparison of findings from Phase 2 and Phase 3. Based on this, the control framework to address information leakage through OSN will be developed as the expected output of this study. The control framework will be validated by doing focus groups to obtain the information security experts' feedback on the framework prior to confirming the final outcome of research.

6 CURRENT STAGE OF THE RESEARCH

The candidate has been writing her literature review, co-writing papers for conferences and journals, has finished the first stage of data collection (to answer the first research question) and is preparing for the data analysis before undertaking the second stage of data collection (to answer the second research question).

7 PLANS FOR COMPLETION

This research commenced on 5th October 2009 and expected to complete in October 2012. It has been and is planned to be carried out based on the schedule presented in Table 1 below.

Research Activities/Milestones	Dates		Duration
	From	To	
Contextual Study Stage	October 2009	August 2010	11 months
- Literature Review - Develop Research Question and Research Objective - Research Design Specifications - Empirical investigation planning - Present at the OASIS research group seminar - Present at the DIS Doctoral Consortium 2010 - Prepare & send research proposal to ACIS Doctoral Consortium - Prepare & send a paper to ACIS Conference - Prepare & send a paper to SECAU Conference			
PhD Confirmation Stage	September 2010	October 2010	2 months
- Preparing for confirmation - Confirmation revision based on feedback - Conversion to PhD program			
Empirical Study Preparations	November 2010	January 2011	3 months
- Planning and preparing for case studies investigation and interview questions - Ethics formulation and approval			
Qualitative Investigation Phase	February 2011	March 2011	2 months
- Conduct first stage of data collection in Malaysia - Prepare and send a paper to a journal			
- Data analysis & report writing - Prepare & send research proposal to PACIS 2011 Doctoral Consortium - Prepare & send a paper to a conference	April 2011	July 2011	4 months
- Revise data analysis & report writing - Conduct second stage of data collection in Malaysia	August 2011	October 2011	3 months
- Data analysis & report writing	November 2011	January 2012	3 months
- Thesis write-up and draft submission - Prepare & send a paper to a conference and journal	February 2012	October 2012	9 months

Table 1. Research Timeline

8 EXPECTED CONTRIBUTION

Existing studies on information disclosure in OSN typically revolves around personal information of end users especially among college students which address the privacy issues of OSN on individuals (Boyd & Ellison, 2007; Christofides et al., 2009; Gross & Acquisti, 2005). However, to date, there are little significant studies concerning OSN impacts on organizational information security. Hence, this study seeks to fill in this gap and contribute to the information systems research community since information security research in information systems is still in its infancy (Zafar & Clark, 2009).

As for the contribution to practice, the recommended information security control framework can be used by organizations to effectively manage and protect their information from unauthorized disclosure through OSN. The control framework, which is expected to include a comprehensive and well-enforced information security policy, and a well-designed and thoroughly implemented security education, training and awareness (SETA) program, and monitored use of preventive systems, would be able to control employees' OSN use behaviour and consequently safeguard organizational information from leakage.

References

Ahmad, A., Ruighaver, A. B., & Teo, W. T. (2005, 21-24 Nov. 2005). *An Information-Centric Approach to Data Security in Organizations.* Paper presented at the TENCON 2005 2005 IEEE Region 10.

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

Boyd, D., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1).

Carvalho, V., Balasubramanyan, R., & Cohen, W. (2009). *Information Leaks and Suggestions: A Case Study using Mozilla Thunderbird*. Paper presented at the CEAS 2009 - Sixth Conference on Email and Anti-Spam.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *Cyberpsychology and Behavior, 12*(3).

CISCO. (2008). *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*. 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*.

DiMicco, J., Millen, D. R., Geyer, W., Dugan, C., Brownholtz, B., & Muller, M. (2008, November 8-12, 2008). *Motivations for Social Networking at Work.* Paper presented at the CSCW '08, San Diego, CA.

Everett, C. (2010). Social media: opportunity or risk? *Computer Fraud & Security,* 8-10.

Facebook. (2010). Facebook Statistics. Retrieved 20 December 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

Goodchild, J. (2010). Social Media Risks: The Basics. *CSO Security and Risk*.

Gross, R., & Acquisti, A. (2005). *Information Revelation and Privacy in Online Social Networks (The Facebook case).* Paper presented at the ACM Workshop on Privacy in the Electronic Society (WPES), 2005, Virginia, USA.

Gudaitis, T. (2010). *The Impact of Social Media on Corporate Security: What Every Company Needs to Know*: Cyveillance, Inc.

Herath, T., & Rao, H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106-125.

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

Mayfield, A. (2008). What is social media?, Available from http://www.icrossing.com/research/what-is-social-media.php

McKenna, B. (2009). Awareness training 2.0. *InfoSecurity,* 18-21.

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior, 26*, 406-418.

Proofpoint. (2009). *Outbound Email and Data Loss Prevention in Today's Enterprise*. California.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*. Paper presented at the Conference on Computer and Communications Security.

Rose, S., Chandramouli, R., & Nakassis, A. (2009). *Information Leakage Through the Domain Name System*. Paper presented at the Cybersecurity Applications & Technology Conference For Homeland Security.

Smith, A. M., & Toppel, N. Y. (2009). *Case study: Using security awareness to combat the advanced persistent threat.* Paper presented at the 13th Colloquium for Information Systems Security Education (CISSE), University of Alaska, Fairbanks, Seattle.

Sophos. (2010). *Security Threat Report: 2010*. Boston, Massachusetts: Sophos Group.

Straub, D. (1990). Effective IS Security. *Information Systems Research, 1*(3), 255-276.

Stutzman, F. (2006). An evaluation of identity sharing behavior in social network communities. *International Digital Media and Arts Association 3*(1), 10-18.

Taylor, S., & Todd, P. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*(2), 144-176.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Society 24*, 472-484.

Verizon, & USSS. (2010). *Data breach investigations report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service*: Verizon.

Workman, M., & 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), 212-222.

Young, K. (2010). Policies and procedures to manage employee Internet abuse. *Computers in Human Behavior, 26*, 1467-1471.

Zafar, H., & Clark, J. G. (2009). Current state of the information security research in IS. *Communications of the Association for Information Systems, 24*(34), 572-596.