Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2011 Proceedings

Australasian (ACIS)

2011

Disclosure of Organizational Information by Employees on Facebook: Looking at the Potential for Information Security Risks

Nurul Nuha
International Islamic University, nurulnuha@kict.iium.edu.my

Abdul Molok
International Islamic University - Malaysia, abdulmolok@pgrad.unimelb.edu.au

Disclosure of Organizational Information by Employees on Facebook: Looking at the Potential for Information Security Risks

Nurul Nuha Abdul Molok
Department of Information Systems
Faculty of ICT
International Islamic University Malaysia
Email: nurulnuha@kict.iium.edu.my, 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

Online social networking (OSN) is a global phenomenon and its use by employees has been reported to be detrimental to organizations. Nevertheless, OSN impacts on organizational information security are rarely discussed in academic literature. This study investigates the use of OSN sites by employees and work-related information disclosed on their personal pages that may jeopardize the security of organizational information. The paper presents the characteristics of work-related information that can be disclosed on Facebook, possibly has the potential to open the doorway for information security threats. It also discusses the qualitative findings from four Malaysian-based organizations under study. Across these four organizations, 22 employees who were active users of Facebook were interviewed to obtain their OSN experience, to explore information they disclosed online and the underlying reasons for doing so. The findings will facilitate our recommendation for organizations to minimize this issue by understanding the behavioural facets of information security.

Keywords

Information disclosure, information security, online social networking, social media

INTRODUCTION

People like to talk about work, to share with their friends about the things that they do for living. However, the conversation that was once personal, momentary and confined to those who heard the conversation, can now be publicly accessed by the whole world, indexed by Google, archived for a long time and could be virtually permanent (Schneier 2009). Thus, organizations are worried about confidential and sensitive information being disclosed to the public domain, thanks to online social networking (OSN) and its users' careless postings (Gaudin 2009; Sophos 2010; Wilson 2009).

While using OSN sites in this ubiquitous world, it is difficult for users to set "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, cases of inadvertent leakage of organizational information have been reported in the media. For example, the Israeli soldier disclosed the military operation through his Facebook profile (BBC 2010) and UK Military secrets being leaked 16 times via Facebook and Twitter (Mansfield 2010). Similarly, the U.S. House Intelligence Committee member, exposed his secret trip to Iraq when he 'tweeted' his arrival in Baghdad using his mobile and continued posting his whereabouts and the party's itinerary every few hours (Ng 2009). And these are just to name a few. If these cases could be done by security-trained personnel, what about those who are not?

Research on Facebook shows that employees are putting too much information on their sites, and, are usually not careful about accepting friends' requests and, using games and other third party applications (Athanasopoulos et al. 2008; Gross and Acquisti 2005; Jagatic et al. 2007). Some users simply accept friend requests to have higher number of friends within their social networks possibly to indicate their popularity. They are not aware that the 'friend' that they added could be a malicious attacker who is conducting surveillance and collecting intelligence on their employer organizations. These attackers can develop and upload applications that contain malware (malicious software) crawling inside users' computing platforms to steal information, sabotage the organization's network, or use organizational resources for launching attacks (Athanasopoulos et al. 2008; Everett 2010; Leitch and Warren 2009). To make it worse, Facebook profiles are now available to be downloaded from torrent sites exposing more than 170 million users' information globally (Paul 2010). Facebook applications are even reported to be sharing personal information of users and their friends with the advertising and Internet tracking companies even if strictest privacy settings had been set (Steel and Fowler 2010). 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 every few minutes (McKenna 2009).

Nowadays, OSN has become a global phenomenon and its use among employees may affect information security in the organizations. Hence, we seek to explore the answers to the research question: Why do employees disclose sensitive organizational information on their OSN sites? Our objectives are to:

1. explore the OSN use behaviour among employees that can risk organizational information security
2. comprehend the reasons for employees to disclose confidential and sensitive organizational information

The main objective of this study is to identify and understand a range of factors that influence employee decisions to disclose information. Among these factors are the security policy document and the extent to which it has been operationalized in the organization, the organizational culture which may or may not be compatible with security objectives, the security awareness and training of employees and a number of circumstantial factors which all contribute to patterns of information disclosure in organizations. OSN is a new platform for information disclosure which poses a unique challenge for organizations seeking to control information disclosure amongst employees. With the understanding of the underlying factors that cause employees to disclose private information to the public domain, we offer our suggestions for organizations to address this issue.

The paper starts with the types of organizational information that can be made available on Facebook. Next, it provides the kinds of organizational information that needs to be protected. The types of information allow us to define work-related information that can be disclosed by employees on social media in the section afterward. In the subsequent sections, we present to you the methodology that was used to undertake the study and then the findings. Finally, we conclude our findings in the Discussion and Future Research section, pointing at the direction for further research in the area.

ORGANIZATIONAL INFORMATION DISCLOSED ON FACEBOOK

This study investigates the different kinds of organizational information that could be disclosed on employees' OSN sites that have the potential to cause information security threats to organizations. Thus, it is important to define the meaning of work-related information in order to provide a clear direction to conduct this study. In order to do that, the review of literature on information disclosure within OSN, information security and information systems (IS) domains was carried out. This section summarizes the findings.

Nosko et al. (2010) describe work information that is disclosed on Facebook as: profile picture about work, information on employer, job position (include previous jobs), job description, location as in city/town, time period and photos about work. As the result of their study, the most disclosed types of work information are information about employer, job position, job description and time period of working (Nosko et al. 2010). Further, they group categories of disclosed information into default/standard information, sensitive information and potentially stigmatizing information, to examine information that would be related to identity, personal and group threats. Their results demonstrate that email, employer, job position, photo albums and tagged photos are categorized into sensitive information.

They identified potential pieces of information that could be included in a profile by examining a blank template of a Facebook profile. Since this was done in 2009, the current settings of a Facebook profile needs to be re-examined should there be more types of work-related information that could be revealed. Hence, we signed up a new Facebook account and took a screen shot of potentially disclosed employment information in the step-by-step registration process. At the time of writing, the following are the identified potential work-related information that could be disclosed by employees in their profiles (Info page – Work and Education): 1. Employer, 2. Job position, 3. Work Location - City/Town, 4. List of Facebook friends who are also colleagues in the same organization, 5. Job Description, 6. Time period – duration (Month, Year) to (Month, Year), 7. Project, 8. Colleagues who are involved in the project, 9. Project Description and 10. Time period – duration (Month, Year) to (Month, Year). Despite these information, users are free to upload as many photos as they want, including photos about work and they can tag their colleagues who are in the photos.

As an addition to Nosko et al. (2010)'s study, the work information that can be published on a profile is information about a user's friends who are also their colleagues or former colleagues, the project(s) that the user is or was involved in, the description of each project and the people who are or were involved in the project.

Although the above information may seem harmless and may give benefits to employees in terms of future work prospects, the disclosure might also lead to information security issues such as leaking confidential information about a project and providing information to someone who is performing information gathering about the organization (Smith and Toppel 2009; Sophos 2010). As Symantec (2011)'s Internet threat report points out,

> *"it is often a simple task for an attacker to discover a company's email address protocol (e.g., firstname.lastname@company.com) and, armed with this information along with any other personal information exposed on the victim's profile, create a convincing ruse to dupe the victim." (Symantec, 2011, p.9)*

Since many users engage on OSN during their routine internet activities, these sites could become a key source of intelligence. Threat agents can launch targeted attacks on organizations and individuals by using spam (unwanted electronic messages), phishing (attempting to obtain sensitive information) and malware through OSN applications (Smith and Toppel 2009; Sophos 2010). Given what cyber criminals already knew, the disclosed information about work provides more insight for them to launch the attacks. Therefore, it is important to look at the types of information that organizations should protect in order to identify the potential risks to organizational information security.

INFORMATION THAT NEEDS TO BE PROTECTED BY ORGANIZATIONS

As employees share their work information with friends and others, social networking sites may open the doorway for information security threats. This section provides the types of confidential and sensitive information that need to be protected by organizations from being disclosed by their employees.

In an article about industrial espionage, Hinson (2010) mentions that it is important to instil awareness among employees to appreciate the value and sensitivity of organizations' tangible and intangible proprietary information. Organizations should enhance security controls to safeguard trade secrets and proprietary information against the efforts of cyber criminals who set out to steal and exploit them (Hinson 2010). He describes the examples of trade secrets and proprietary information that could be carelessly revealed by employees via online social media as:

1. Information about costs, prices, profitability
2. Production processes
3. New products under development
4. Corporate strategies

In similar vein, Information Security Forum (ISF) (2007) in an article about information leakage, reports that employees may place details of business projects on a blog or community websites such as LinkedIn or Facebook. This can be done as the result of an unintended action and it can be linked with malicious intent. The details could be read by a competitor, risking the organizational information security (ISF 2007). The article presents the examples of confidential and valuable information as follows:

1. information that is of strategic importance (mergers and acquisitions plans, which would be of interest to competitors)
2. information that contains personal details (customer information that could be news-worthy to media organisations)
3. information that consists of trade secrets or intellectual property and is commercially sensitive (product plans that could be useful to competitors)
4. information that appears embarrassing or libellous (statements about business partners that could be used in legal proceedings)
5. information that is subject to legal and regulatory requirements (personal data protected by laws such as EU's Data Privacy Act or US' Gramm-Leech-Bliley Act)

In another study about organizational secrets (Anand and Rosen 2008), the authors outline the following as the examples of organizational secrets: employee salaries, product formula and medical records. However, Forrester (2010) illustrates two types of enterprise information that Chief Information Security Officers wish to protect: corporate secrets and custodial data. Corporate secrets are information that gives long-term competitive advantage such as strategic and product plans, earnings and financial forecasts, and trade secrets. Custodial data includes customer's personally identifiable information such as name, address, email, and phone number; payment card details like credit card numbers and expiration dates; medical records and government identifiers like passport number (Forrester 2010).

Now that we know the types of organizational information which have the potential to be disclosed on Facebook and the kinds of information that need to be secured by organizations, these information types are able to help us define work-related information that we want to look for in our study.

THE DEFINITION OF WORK-RELATED INFORMATION

The different types of information in different domains of study assist us to characterize work-related information that could be revealed by employees on their OSN sites particularly Facebook. Before we define work-related information, it is interesting to look at a study of information types (Shaari et al. 2008) and defining information (McKinney and Yoos 2010) within the IS field.

Shaari et al. (2008) present the taxonomy of information types being exchanged by the members of virtual teams (VT) and how information influences VT functioning. They classify nine types of information which are information about tasks, members, team, ICT, external working environment, clients, external resource network, organization context and meta-information.

According to McKinney and Yoos (2010), while information is one of the most fundamental terms in sciences, linguistics and economics, it is poorly defined in the IS literature. Hence, they present the taxonomy of information from the view of token, syntax, representation and adaptation (McKinney and Yoos 2010). We concur with the definition of information from the representation view which states that information is meaning and a model of something to someone. It consists of a sign, an object and an observer; the authors explain that an observer understands an object based on a sign. For example, personal information (sign) about an individual (object) gives meaning to a third party (observer) based on the observer's knowledge. Likewise, information that is posted on OSN sites would be interpreted by different observers differently based on the observers' knowledge. Hence, information disclosure on OSN could be interpreted as beneficial by someone at the same time problematic to someone else which denotes the worthiness of research to investigate the positive and negative sides of OSN.

The positive sides of OSN are it is vastly used by companies to advertise new products (Tikkanen et al. 2009), a platform to make employment selection decisions (Kluemper and Rosen 2009), a new method of communication between colleagues (DiMicco et al. 2008) and it has the potential to be appropriated and repurposed to support teaching and learning in higher education (Hamid et al. 2010). On the other hand, OSN can open the doorway for many information security threats such as an avenue for cyber espionage (Smith and Toppel 2009; Sophos 2010), botnet (a collection of compromised computers) attacks (Athanasopoulos et al. 2008; Leitch and Warren 2009) and damaging reputation of an organization due to inappropriate contents disclosed by employees (Colwill 2010; Wilson 2009).

However, this study takes a more neutral stance to examine the types of work-related information that might be revealed by employees before confirming the issues that information disclosure on OSN might bring to organizational information security. In order to do that, the definition of work-related information is given based on the review of literature on information disclosure from multi-discipline domains given in the previous section. By combining the information about work that could be disclosed on users' Info page on Facebook, and studies by Hinson (2010), ISF ((2007), Forrester (2010) and Shaari et al. (2008), we present the types of work related information that have the potential to be disclosed by employees on OSN sites:

Table 1. Work Related Information that could be disclosed by employees on their OSN sites

	Type of information
The organization	Background and location Strategic plan The management team Corporate Policy Culture of the workplace Events
Job description	Background, time period Progress Output Problems encountered

Colleagues	Background Tasks or projects they are involved in Success, Failure
Products or services	New products or services Production processes Costs, retail prices, profits
Clients	Personal information, expectations
Third parties	Business partners, suppliers, consultants

In a nutshell, we define work-related information that can be disclosed on social media as the information about the organization, job tasks, colleagues, product/services, clients and third parties.

RESEARCH METHODOLOGY

This study utilized a qualitative research approach by using multiple case studies method and interviews as data collection instrument. The interview questions were designed through the lens of Taylor-Todd's Decomposed Theory of Planned Behavior (DTPB) that provides the understanding of the underlying reasons why users employ an information system (Taylor and Todd 1995), in this case, social media. The DTPB theoretical model and its relation to information leakage through OSN were discussed in great length in our previous paper (Abdul Molok et al. 2010a). The theoretical model was also used in guiding the data analysis of this study.

Multiple case studies were carried out on four organizations in Malaysia; a tertiary education provider, an agency responsible for managing ICT, an organization that regulates the communication industry, and an information technology (IT) security service provider. A total of 22 employees across the organizations were interviewed from February to March 2011. The invitation to participate in the research was sent to the organizations and it was forwarded to the employees. In each organization, we managed to get five to six employees who were interested to participate in the study.

Before the interview, the participants were asked to fill up a short survey (a single page which contains six questions) about basic OSN use. They were then interviewed in front of their Facebook pages to understand how they engaged in OSN activities and why they disclosed certain types of information on their sites and their friends' sites. Each interview took about 45 minutes to 60 minutes.

With their permission, after the interview, we further observed the kinds of information that they disclosed on their OSN sites for a short period of two weeks. We used the observation to justify their answers during the interviews.

FINDINGS

The qualitative data were analyzed using thematic coding (Lee et al. 1999). The findings of this study were focused on how and why the participants used Facebook to communicate with their colleagues, the types of work-related information they shared online, and the reasons behind this behavior.

Generally, 100% of the participants used Facebook and 73% of them used Facebook several times a day. Other social networks sites they used are Twitter (18%), MySpace (14%), Friendster (9%) and Tagged and LinkedIn (both 5%). Hence, the rest of the findings were based on the use of Facebook.

Using Facebook

All participants used Facebook on a regular basis at work, home and/or using mobile devices. 91% of participants used Facebook both at work and at home, with 64% using their mobile devices to access Facebook. However, 36% of participants never used their mobiles to access Facebook mainly due to the inability of their mobile phones to access the Internet. The Facebook activities that were used by all participants were viewing friends' postings (with 59% of participants doing it several times a day), commenting on friends' postings, sharing their current status, sharing photos and sending messages to friends. More than half of them shared external links with their friends (mostly links from YouTube and news agencies), played games (Farmville, Mafia Wars etc) and used other third party applications (IQ Test, Family Tree etc).

For the purpose of using Facebook, we found that all participants used Facebook to keep in touch with friends, 59% used it to stay in touch with family members, and 41% to make new friends. Interestingly, 45% discussed work with colleagues and 18% of the participants used Facebook to perform job tasks. Some of the tasks that they talked about were to make announcements to colleagues (and also to students for the university case), update the organizations' Facebook pages to promote their organizations, services and events, and, to monitor employees' Facebook activities and do investigations on the contents. This means that employees did not only use Facebook for personal matters but also to discuss work with colleagues and carry out tasks. Since some of the participants used Facebook to monitor and investigate its contents, it shows that, in some cases, organizations had mitigating actions on OSN use within the work environment.

Regarding the mitigating actions on OSN use within the work environment, it is important to note that some employees used Facebook for work purposes outside the work environment. This is because all participants stated that they accessed and used Facebook outside office hours using their smart phones and home computers, as in some organizations, the access to Facebook and other social media during office hours was restricted. On the other hand, 15 out of 22 of them stated that they used Facebook during office hours for work and personal purposes, which indicate the issue of productivity among employees.

Keeping in touch with colleagues

Since this study focuses on work-related information disclosure on Facebook, we focused on the participants' communication with their colleagues. Generally, participants communicated with colleagues about meetings, tasks, celebrations, commiserations and frustrations. One of the participants mentioned that, *"Let's say someone just attended a meeting, and I have no time to meet the person, I would ask him/her what the meeting was about (on Facebook). When I see the person online, I will use chat to ask him/her."* Some participants also revealed they used wall updates to remind colleagues about meetings. When asked why meetings reminders were posted on the wall, one of them said *"Because many colleagues are online on Facebook. If I send (the reminder) through email, some do not check their emails that often".* Others used Facebook to obtain fast response from colleagues about tasks, to congratulate colleagues on their promotion, to bid farewell to colleagues who were leaving the organizations, to have lunch with colleagues, to inform colleagues that they were on leave and to find people for their boss.

In quite a similar manner, most participants from a university informed that Facebook makes their jobs easier to locate students in order to form alumni, to communicate with current and potential students about research projects, to assist students to get job opportunities, and to make announcements to colleagues and students. A lecturer mentioned, *"In the office I usually use Facebook to find students. Recently we wanted to create ABC Alumni, so where to find them? On Facebook… We could not find them in the University database, probably the information in there is not updated. To send them a letter would take time. So we used Facebook and we found 80% of the ex-students through Facebook. We sent them a message then they replied. It was much faster".*

About 30% of the participants used Facebook to promote and advertise the organization's services and events. As one of them mentioned, *"Sometimes I do share some information from that page (company Facebook page) and put it on my wall".* In some cases, the organizations maintain 2-3 Facebook pages to reach and provide information and news coverage to customers.

It is imperative to note that each participant informed that they had seen posts about frustrations at work on colleagues and friends' wall, typically expressing their dissatisfactions about the boss, colleagues, workloads and clients. One of them admitted on posting on his wall about being disappointed with a colleague who did not contribute in an important task. He received responses from colleagues who understood his situation and offered him moral support. Another mentioned, *"Some of them (colleagues) do not even set their privacy settings, so I could still see their pages without being their friend on Facebook. I have seen some of them complained about work. We know them, so we know who they were talking about".* There was even a Facebook post to express dissatisfaction with clients, "*she posted her frustrations about her clients. It was not obvious, but you can tell that she is having a problem with her clients".*

Types of work-related information shared publicly

As shown in Table 1, the types of work-related information that employees could disclose on Facebook are the information about the organization, job tasks, colleagues, product/services, clients and third parties. By communicating with colleagues and friends on Facebook about meetings, tasks, celebrations, commiserations and frustrations at work as described in the previous subsections, we found out that the types of work-related information that were disclosed are information about the organization, superiors, colleagues, clients, events and tasks. Additionally, we also found some participants shared with friends work photos of bosses, colleagues and guests (some high profile guests or VIPs) during company events.

For the information about the organization, 15 out of 22 participants did not disclose the name of the organizations that they worked at in their Facebook Info page. This was because they did not want their friends to know their employer and their job description. Some of them informed that they did not want to mix personal life with work. However, seven of them did disclose the job position and employer information on their profile. Other than that, some participants used Facebook to inform friends about the organizations' location, job application, organizations' events and as stated earlier, information about organizations' background, news coverage and services.

As mentioned above, some employees posted their frustrations about the boss while some others posted photos taken with the boss. However, some of the participants informed that they would not disclose any information about their superiors, as one of them said, *"My friends know where I work at, but I prefer them not to know that I am working for a particular man. If they do, I might be put in a difficult situation where… they want an appointment to meet with him (the boss), …they want me to help them."*

As for information about colleagues, participants pointed out some information regarding complaints about colleagues, playing Facebook games to compete with colleagues and photos taken with colleagues during lunch and at the company events. During the interviews and observations on participants' Facebook pages, we encountered many photos taken with colleagues at company's events. One of them said, "*…all of us were wearing nice outfits and glamorous, I took their photos and tag them. But for me, when people tag my name, I will choose the photos, if I think I don't like it, I will remove the tag myself*" and another mentioned, *"I uploaded photos taken at our company dinner during speeches, prize giving, singing performance and while eating"*.

About photos, indeed, a picture speaks louder than words. Hence, some of the participants were careful about posting photos of their bosses and high profile guests at the company events on Facebook. When asked why, one of them said, "*Putting up photos of your boss, some ministers, draws a lot of attention from others. Whether they want to use the information in a good way or bad way, you'll never know. Actually whatever information that you post and whatever photos that you upload, there is a risk behind it."* Nevertheless, some of them mentioned that there were colleagues who were proud to have taken photos with their superiors, ministers and government officials. It becomes an issue when comments that were made by some friends on the photos could cause negative impacts, as told by one of the participants, *"To me these photos are not meant for others. Some put up nasty jokes on photos taken with the wife of the ministers like who is fatter than the other. To other people, this could be sensitive, although to us it was just a joke."*

Facebook and other social network sites provide the platform for users to share information about anything with the people within their social networks; colleagues, current friends, old friends, family, members of interest groups and friends-of-friends. People are free to respond to whatever information being posted on these sites. Some comments from friends may give comfort and some others may be a discomfort as postings being misinterpreted by others as mentioned by some of the participants. However, some "friends" may be a malicious attacker lurking inside users' profiles to gather intelligence in order to launch a targeted attack. The attacks could be backstabbing, identity theft, social engineering, corporate espionage and sabotage. More information about this was covered in our security paper (Abdul Molok et al. 2010b).

The reasons behind the disclosure

When we asked the participants why did they think some people mindlessly disclose sensitive things about themselves and others on Facebook, these are some of their answers:

1. Feeling better once they have expressed their feelings

   "I think it (Facebook) is the platform to express their feelings and relieve distresses in life"

2. Being influenced by their friends

   "I have a friend who follows what other friends do. People post frustrations, she will do the same"

3. Getting support from friends

   "If advice is required maybe that is their way of sharing (problems) with their friends."

4. Being unaware of the consequences they might face

   "There are some users who don't know how to really use Facebook and just know the basic functions. This is a problem. Some people think that social media is a free thing so they freely post many things on the sites, things that they won't say in person, in face-to-face but they make it possible there (on social media). Maybe they don't know whatever they post can be read by a lot of people"

5. Being addicted to Facebook

   "I cannot deny that Facebook is like a disease which has spread so quickly, it is very addictive, probably every person that you bump into has a Facebook page. If you cannot access it at work, you can access through your mobile. There are so many other ways. If you have a USB broadband, you can just plug it in, you can still access it."

It is human nature for people to share what they do with others, and to err is human. Some participants pointed out that there were times that they wished they could undo certain things they did on Facebook. As one of them stated, *"When I was a heavy user, I opened a lot of things about myself which I should not"*. People may forget face-to-face conversations, however, postings on Facebook are instant and possibly permanent, and even if the postings were later deleted, some people may have read them and the information may be archived (Schneier 2009; Sophos 2010; Symantec 2011). The disclosure of confidential information about work on Facebook may jeopardize the organization's reputation and the damage could have already been done the moment an employee posted it, whether accidentally or intentionally. It is most likely being realized only when the organization and the employees have suffered the consequences. Perhaps, organizations and individuals need to understand the consequences in order to minimize this issue.

DISCUSSION AND FUTURE RESEARCH

Our initial findings through the literature guided the formation of the characteristics of work-related information that we investigated on employees' Facebook pages. Hence, in this context, we defined work-related information as the information about the organization, job tasks, colleagues, customers, product/services and third parties as presented in Table 1. Through our findings of empirical data, we found that the types of work-related information that were disclosed by the participants are information about the organization, superiors, tasks, colleagues, clients, events and some high profile people who happened to be the guest-of-honor at company events.

We are in no position to say which information is confidential, which one is sensitive and which one is not. It depends on the organizations to decide for themselves based on their nature of business, although frequently organizations cannot tell how information might be used against them. Therefore, in the next study, we will return to the organizations under study, present to them our findings, and discuss with them the information disclosed by their employees that are considered non-stigmatizing, potentially stigmatizing and confidential.

As some information security risks due to Facebook use, such as distribution of malware through games and applications, may be minimized using network monitoring and preventative systems installed within the corporate networks, confidential information disclosure is difficult to contain. Furthermore, some employees use Facebook to discuss work outside of the work environment. As mentioned by one of the participants who happened to be the security analyst in one of the organizations,

> *"From our department's view, by using the existing systems, we can control Facebook users who are playing games, downloading applications, uploading photos etc, but when it comes to the disclosure of confidential organizational information, it is difficult to prevent. They can access Facebook wherever they are and they can use their mobile phones to do that. In this case, I think security awareness and monitoring should take place. Somebody could proactively monitor Facebook use among all employees, but that is a very tedious job. In the office, yes we can monitor, outside the organization, it is difficult. I think the biggest threat is the use of Facebook through mobile phones, people can do it in real time, wherever they are, they can post anything, or take a picture using their mobile phones and upload them right away. Before we can do something about it, the damage could have been done."*

Hence, we propose the understanding of OSN use behavior among employees in order to minimize the information security risks the behavior might bring to organizations. This is because many organizations lack the understanding of the ever changing social networking threat landscape in order to make critical decisions regarding OSN use (Websense, 2010). Our previous study showed that the possible mitigating actions to minimize information security threats through social media are information security policy that is implemented thoroughly and well-enforced, security education, training and awareness (SETA) and preventive systems (Abdul Molok et al. 2010b). However, which mechanism can reduce this issue effectively and efficiently? Perhaps we can infer the following from what we did not see in the organizations and what we did not hear from the participants:

Poor decision-making

Some of the participants showed that when they and their colleagues used OSN, their decisions regarding information disclosure were made as if they were not informed by organisational guidelines. This is because we did not see employees consulting organisational guidelines (or being aware of organisational guidelines or where they might be found) when deciding whether to divulge particular information which implies the organisation seems to have no official or formal policy or guidelines to advise their employees as to what is appropriate behaviour on OSN.

Misdirected Security Strategy

The findings showed that security administrators in the organizations under study were still fixated on technical solutions rather than focusing on how to control the behaviour of their employees. This was shown when security staff referred to technical controls while they acknowledged that employees access social networking sites using personal as well as organisational technology. One of the participants who happened to be the network administrator in one of the organizations pointed out when asked about the use of mobile phones to use Facebook, *"Users are free to use their personal devices. Our concern is more on the security of our local network, we don't want our network to be tampered with."*

Inadequate measures to protect sensitive information

Academic literature and our findings suggest that organizations have not pro-actively identified the kinds of information that are 'sensitive' and have not implemented measures to protect those kinds of information from accidental disclosure. Some administrators did not refer to any policy or document that identifies and classifies or categorises organisational information based on sensitivity.

Inadequate measures to educate and train employees that routinely access sensitive information

Some of the participants informed that administrative staff tend to be unaware about social media use and information security compared to the technical staff. However, administrative staff are often entrusted to deal with organizational information. Moreover, in some organizations, they have not recognized that levels of access to sensitive information increase the likelihood of disclosure. There was no indication from administrators that special measures were in place for senior management or for administrative staff with access to sensitive information.

We found in the study that there is no all-encompassing technical solution to the problem of confidential and sensitive information disclosure through OSN. Any strategies that focus purely on denying access to employees is misdirected as users will use OSN outside the organisational environment. If organisations are to effectively mitigate the risk of information disclosure then the focus must include changing the behaviour of employees especially influencing their decisions and decision making process. However, it is clear that organisations have not done their own homework on the problem of information disclosure. There is no evidence that organisations have identified the range of sensitive information that exists and/or provided guidelines or advice to employees on information disclosure (on OSN or through any other medium). A key element of an effective policy would be to recognise that the risk of information disclosure is not the same for all employees and that high-risk categories such as senior management, administrative and legal staff etc. require additional security education, training and awareness (SETA).

Thus, we call for more research to understand human behavior in order minimize information security incidents. Perhaps SETA programs for employees are a promising way to address this issue as some IS security scholars stated that they play a key role in employees' information security compliance behaviour (Bulgurcu et al. 2010), improves employees' behaviour, and enable organizations to hold employees accountable for their actions (Whitman and Mattord 2008) and increases employees' perceptions of vulnerability and severity of information security threats (Workman and Gathegi 2007).

CONCLUSION

Our research demonstrates that employees disclose work-related information that has the potential to incriminate organizational information security. This will be further confirmed in our next stage of study by returning to the organizations under study and identify the types of information that are potentially stigmatizing and confidential. Frequent use of OSN particularly Facebook among employees allows work-related information to be shared in and out of the work environment. This means that the potential for organizational information to be leaked can happen outside the work environment. Therefore, security measures that are strategy and structurally focused are inadequate. It is just as important to look at a culture change of employees' OSN behaviour. Since employees often unthinkingly post information, not realizing that the information is stored and searchable by other people, we call for more research into OSN use behaviour among employees for organizations to minimize information security risks.

This study offers contributions to the IS security research and practice. It addresses the research gaps concerning the behavioural aspects 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

Abdul Molok, N.N., Ahmad, A., and Chang, S. 2010a. "Understanding the Factors of Information Leakage through Online Social Networking to Safeguard Organizational Information," *21st Australasian Conference on Information Systems (ACIS2010)*, Brisbane, Australia: Association of Information Systems.

Abdul Molok, N.N., Chang, S., and Ahmad, A. 2010b. "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats," *8th Australian Information Security Management Conference,* D.C. Bolan (ed.), Perth, Western Australia: Security Research Centre, Edith Cowan University.

Anand, V., and Rosen, C.C. 2008. "The Ethics of Organizational Secrets," *Journal of Management Inquiry* (17:2), pp 97-101.

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

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp 523-548.

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., and Muller, M. 2008. "Motivations for Social Networking at Work," *Computer Supported Cooperative Work (CSCW'08)*, San Diego, California: ACM.

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

Forrester. 2010. "The Value of Corporate Secrets," Forrester Research, Inc., Cambridge, Massachusetts.

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.

Hamid, S., Waycott, J., Kurnia, S., and Chang, S. 2010. "The Use of Online Social Networking for Higher Education from an Activity Theory Perspective," *14th Pacific Asia Conference on Information Systems (PACIS 2010)*, Taipei, Taiwan: Association of Information Systems.

Hinson, G. 2010. "Industrial Espionage," in: *NoticeBored Newsletter*. Hastings, New Zealand: IsecT Ltd., pp. 1-7.

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

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

Kluemper, D.H., and Rosen, P.A. 2009. "Future Employment Selection Methods: Evaluating Social Networking Web Sites," *Journal of Managerial Psychology* (24:6), pp 567-580.

Lee, T.W., Mitchell, T.R., and Sablynski, C.J. 1999. "Qualitative Research in Organizational and Vocational Psychology, 1979–1999," *Journal of Vocational Behavior* (55), pp 161-187.

Leitch, S., and Warren, M. 2009. "Security Issues Challenging Facebook," *7th Australian Information Security Management Conference,* C. Bolan (ed.), Perth, Western Australia: Edith Cowan University, pp. 137-142.

Mansfield, R. 2010. "Uk Mod Secrets Leaked onto the Internet." Retrieved January 25, 2010, from http://news.sky.com/skynews/Home/UK-News/Ministry-of-Defence-Staff-Have-Leaked-Secret-Information-16-Times-Onto-Social-Networking-Sites/Article/201001415535304

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

McKinney, E.H., and Yoos, C.J. 2010. "Information About Information: A Taxonomy of Views," *MIS Quarterly* (34:2), pp 329-344.

Ng, V. 2009. "Us Congressman Twitters Secret Trip to Iraq," in: *Search Security Asia*.

Nosko, A., Wood, E., and Molema, S. 2010. "All About Me: Disclosure in Online Social Networking Profiles: The Case of Facebook," *Computers in Human Behavior* (26), pp 406-418.

Paul, I. 2010. "The Facebook Data Torrent Debacle: Q&A," in: *PCWorld*. San Fransisco: PCWorld Communciations.

Schneier, B. 2009. "Special Report: Industry Experts Debate Social Networking Risks," in: *Security Asia*.

Shaari, I., Chang, S., and Shanks, G. 2008. "Virtual Teams: Information Types for Effective Functioning," in: *12th Pacific Asia Conference on Information Systems (PACIS)*. Suzhou, People's Republic of China: AIS.

Smith, A.M., and Toppel, N.Y. 2009. "Case Study: Using Security Awareness to Combat the Advanced Persistent Threat," *13th Colloquium for Information Systems Security Education (CISSE)*, University of Alaska, Fairbanks, Seattle: CISSE, pp. 64-70.

Sophos. 2010. "Security Threat Report: 2010," Sophos Group, Boston, Massachusetts.

Steel, E., and Fowler, G. 2010. "Facebook in Privacy Breach: Top-Ranked Applications Transmit Personal Ids, a Journal Investigation Finds," in: *The Wall Street Journal*. New York, USA: Dow Jones & Company, Inc.

Symantec. 2011. "Internet Security Threat Report Trends for 2010," Symantec Corporation, California, USA.

Tikkanen, H., Hietanen, J., Henttonen, T., and Rokka, J. 2009. "Exploring Virtual Worlds: Success Factors in Virtual World Marketing," *Management Decision* (47:8), pp 1357-1381.

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

Wilson, J. 2009. "Social Networking: The Business Case," in: *Engineering & Technology*. Institution of Engineering & Technology, pp. 54-56.

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.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their useful comments. Nurul Nuha Abdul Molok is a PhD student at the Department of Information Systems, The University of Melbourne. Her PhD education is financed by the Malaysian Ministry of Higher Education and the International Islamic University Malaysia.

COPYRIGHT