Disclosure of Organizational Information on Social Media: Perspectives from Security Managers

Nurul Nuha Abdul Molok
International Islamic University Malaysia, nurulnuha@iiium.edu.my

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

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

Follow this and additional works at: http://aisel.aisnet.org/pacis2013

Recommended Citation
Abdul Molok, Nurul Nuha; Chang, Shanton; and Ahmad, Atif, "Disclosure of Organizational Information on Social Media: Perspectives from Security Managers" (2013). PACIS 2013 Proceedings. 108.
http://aisel.aisnet.org/pacis2013/108
DISCLOSURE OF ORGANIZATIONAL INFORMATION ON SOCIAL MEDIA: PERSPECTIVES FROM SECURITY MANAGERS

Nurul Nuha Abdul Molok, Department of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia, nurulnuha@iium.edu.my

Shanton Chang, Department of Computing and Information Systems, University of Melbourne, Victoria, Australia, shanton.chang@unimelb.edu.au

Atif Ahmad, Department of Computing and Information Systems, University of Melbourne, Victoria, Australia, atif@unimelb.edu.au

Abstract

Despite the benefits of social media to organizations, the pervasive online social networking (OSN) among employees has been reported to be detrimental to organizations. The ubiquity of social technologies makes employees’ professional and personal boundaries unclear, allowing inadvertent leakage of organizational information through the public domain. Without proper information security management, social media could be a double-edged sword to organizations. Hence, some organizations are employing various security strategies to mitigate employees’ use of these social platforms. While cases of information leakage through OSN have been reported worldwide, its coverage in academic literature is scant. This paper aims to fill in this research gap. It reports the findings of a qualitative multiple-case study to unravel information security issues that OSN might bring to organizations. It also describes the security strategies employed by organizations and factors that influenced the strategy decision. The understanding of this contemporary phenomenon and organizational security strategy contributes to the development of a theoretical framework that may offer practical insight to organizations.

Keywords: Online Social Networking, Social Media, Information Leakage, Information Security Management.
1 INTRODUCTION

“The danger of putting too much personal information online, particularly on social networking sites, was brought to light when the wife of the chief of the British secret service MI6 posted highly revealing details about their residence and friends on her Facebook page.” (Sophos, 2010, p.6)

The above incident which happened in July 2009 was the classic example and the turning point for organizations to refocus their online social networking (OSN) concerns on the leakage of organizational information. According to Sophos (2010), prior to this, organizations were more concerned about employees’ productivity and depletion of network bandwidth. After the incident, more similar cases were reported; an Israeli soldier who leaked the location of the military operation on his Facebook page, U.K. military secrets that were revealed 16 times via Facebook and Twitter, and a U.S Congressman who tweeted his secret trip to Iraq via his BlackBerry (Abdul Molok, Ahmad, & Chang, 2011). The advancement of mobile technologies and new functions on OSN applications such as geo-tagging (the process of adding geographical location on images or videos), further escalates such occurrence. As expected, there were even more cases of leakage through Facebook and Twitter that did not make it on the news. One of our samples affirmed that employees were found checking in from their workplaces, and one of them was a military depot.

Despite this pervasive phenomenon that has captured the media’s attention, its coverage in the academic literature is scant. Thus, we attempted to fill in this research gap by conducting contextual study which was published in the 21st Australasian Conference of Information Systems (ACIS) (Abdul Molok, Ahmad, & Chang, 2010) and a security journal (Abdul Molok, Chang, & Ahmad, 2011), and our first empirical study was published in the 22nd ACIS (Abdul Molok, Ahmad et al., 2011). The earlier study investigated OSN behaviour among employees and the types of information about work they disclosed online. This paper presents our second empirical study to understand whether organizations were concerned about such behaviour and whether they realized that leakage of organizational information through employees’ OSN could happen. The main aim of the current study is to investigate the strategies implemented by organizations to mitigate security issues around OSN and the factors that influenced the strategy decision. Hence, this paper seeks to provide answers to the following questions:

1. How do employees contribute to leakage of organizational information through OSN?
2. How do organizations mitigate information leakage through employees’ use of OSN sites?
3. Why do organizations employ certain security strategies to mitigate information leakage through OSN?

This paper starts with the review of literature on information leakage and OSN. Then, it describes the research methodology employed for this study, followed by analysis of data and findings. Finally, it presents the discussion and conclusion of the study.

2 LITERATURE REVIEW

2.1 Information Leakage

Information leakage has been studied for decades as shown by one of the earlier studies done by Katz (1976) about the legal implications of confidential information in government being leaked to the public. He uses the term unauthorized leaks in which he states that an unauthorized leak occurs when an employee publicly discloses information that his or her superior chose not to disclose (Katz, 1976).

Similarly, a more recent article on information leakage from Information Security Forum (ISF) also focuses on leakage of sensitive information made by an employee allowing the public to have access to the information (ISF, 2007). The article describes information leakage as one of the threats to information security, therefore organizations should be aware of the avenues of leakage and what to do to prevent it. The international standard on information security management uses the terms information leakage and unauthorized information disclosure interchangeably in specifying the act of
disclosing information that is not supposed to be disclosed to unauthorized people (ISO/IEC, 2005). Despite these terms, Gross and Acquisti (2005) use the term information revelation to study the patterns of information revelation in online social networks and their privacy implications amongst college students.

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). Leakage of information is one of the insider threats to information systems (IS) that should be addressed by organizations to safeguard their confidential information. This security threat can be caused by human and non-human perpetrators from inside or outside the organization (Loch, Carr, & Warkentin, 1992). It can happen through many different channels such as OSN, face-to-face conversation, printing facilities, email, cloud computing, domain name systems, portable data devices and even offline social networking such as conference and publication (Abdul Molok et al., 2010).

Among these leakage platforms, we view OSN as the most challenging channel of information leakage. The moment information is posted on social media, it can be accessed by anyone, indexed by Google and archived, making it virtually permanent. Information that has been leaked whether intentionally or unintentionally would open the doorway for cybercriminals 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). A more recent study on the OSN security challenges to organizations points out the challenges coming from outside attacks on employees and companies, insider attacks due to employees’ actions and unawareness, and blurring of professional and personal roles (Hekkala, Vayrynen, & Wiander, 2012). Similar to our previous studies (Abdul Molok et al., 2010; Abdul Molok, Ahmad et al., 2011), they describe employees’ action can cause information leakage either accidentally or intentionally. However, while we explored information leakage through OSN phenomenon from the perspectives of both employees and security managers, Hekkala et al. (2012) cover social media challenges to organizations from security managers’ perspective only. Additionally, while we focused on OSN impacts to organizational information security, existing literature covers OSN impacts to security and individual privacy (Besmer, Lipford, Shehab, & Cheek, 2009; Furnell & Botha, 2011; Nosko, Wood, & Molema, 2010; Paquette & Fagnot, 2010).

2.2 Online Social Networking

The use of social media has been proliferating since the creation of the first OSN site, Six Degrees.com launched in 1997 (Boyd & Ellison, 2007). According to Boyd & Ellison (2007), the site allowed the creation of user profiles and inclusion of friends, which led to other social networks sites such as MySpace, Facebook and Friendster that continued to form the professional, social and research landscape. The popularity of these communication platforms made OSN the global phenomenon, especially when Facebook expanded their college networks to corporate networks and finally to everyone. Thanks to the advancement of mobile technologies, users can now expand their networks of contacts, utilize many applications and share information seamlessly, anytime at anywhere. At the time of writing, Facebook is the second most visited site in the world, in United Kingdom and United States, and the top most visited site in Argentina, Malaysia and Turkey, to name a few (Alexa, 2013).

Social media is the new socialization tool in the digital age which consists of social networks (Facebook, LinkedIn and MySpace), microblogging (Twitter), content communities (YouTube and Flickr), blogs, wikis and forums (Mayfield, 2008). Recently, Google+ joined the OSN landscape claiming to provide better security over information sharing (Fowler & Efrati, 2011). Although social media is often epitomised by sites like Facebook, LinkedIn, MySpace and Twitter (Wilson, 2009; Young, 2009), the study focuses on OSN behaviour regardless of the types of media. Hence, adopting Mayfield’s (2008, p.5) definition of social media, OSN in this context is referred to the practice of sharing information and contents on “online social media which share most or all of the following characteristics: participation, openness, conversation, community and connectedness”.
Facebook reached its 1 billion users on 14 September 2012 (Vance, 2012), making it the most popular OSN site worldwide (Heidemann, Klier, & Probst, 2012). While the growth of Facebook captured corporations’ interest to generate their competitive advantage, Facebook is viewed to be the site that poses the biggest risk to security (61%), significantly ahead of MySpace (18%), Twitter (17%) and LinkedIn (4%) (Sophos, 2010). In fact, the widespread adoption of Web 2.0 platforms particularly Facebook lures cybercriminals to use these platforms as the attack vectors (Athanasopoulos et al., 2008; Jagatic, Johnson, Jakobsson, & Menczer, 2007; Leitch & Warren, 2009; PricewaterhouseCoopers, 2010). Hence, many organizations are facing challenges to secure their valuable asset, information. They are concerned with employees’ OSN since this behaviour affects productivity, information leakage, malware and phishing attacks, and provides capabilities for cybercriminals to gain more access to corporate servers through reconnaissance on employees’ OSN sites (Colwill, 2009; Gudaitis, 2010; Hekkala et al., 2012; Smith & Toppel, 2009; Sophos, 2010; Symantec, 2010; Wilson, 2009).

There is no doubt that the use of social media is beneficial to organizations and employees. Organizations worldwide are using these sites to market their products and services, to obtain feedback from customers, to recruit potential employees, to be used as an internal communication platform among colleagues and even to support teaching and learning in education institutions (Abdul Molok, Ahmad et al., 2011). However, the instantaneous and dynamic nature of social media has made it a new platform of information leakage which poses a unique challenge for organizations. Although information can be leaked via many means of telecommunication channels, the pervasiveness of OSN makes it more challenging for organizations to prevent their valuable information from being disclosed to unauthorized parties. Nevertheless, the academic literature seldom discussed the information security impacts of OSN on organizations. Generally, research on social media focused on individual privacy issues, self presentation, network analysis and social capital benefits (DiMicco et al., 2008). Thus, this research aims to fill in this gap with empirical research about the current phenomenon that is affecting organizations globally.

2.3 Strategy to address Information Leakage through OSN

IS security literature proposes information security policy, security education, training and awareness (SETA) and preventive security systems as key deterrents to insider’s threats (Bulgurcu, Cavusoglu, & Benbasat, 2010; Straub, 1990; Workman & Gathegi, 2007). Our work that was published in a security journal already discussed the advantages and disadvantages of each control mechanism (Abdul Molok, Chang et al., 2011). In summary, security policy and acceptable use policy of social media are important in managing organizational information security around employees’ OSN. SETA programs play the role to ensure employees’ compliance to the OSN security policy. Technological control mechanisms may deter external attacks through detection, prevention and mitigating actions.

Management consulting firms are providing their services to advise organizations in managing social media in the workplace (Ernst & Young, 2010; PricewaterhouseCoopers, 2010). Similarly, security providers have already introduced various control mechanisms such as data leakage prevention (DLP), identity and access management (IAM), and web filtering systems in order to control leakage of information (Sophos, 2010; Symantec, 2010). However, not all organizations have the ability to invest a large sum of money to obtain the management consulting services and employ the security systems. Therefore, organizations need to adopt a more practical approach to address security risks around OSN. This is the intention of this paper, to understand the various OSN security strategies implemented in organizations and propose a framework to address this issue.

3 RESEARCH METHODOLOGY

Following Yin’s (2009) multiple-case study design but focusing on Walsham’s (1995) interpretive case study approach, this study employed a qualitative multiple-case study on four organizations (Walsham, 1995; Yin, 2009). Interviews were the primary data collection instrument and document reviews were secondary. We interviewed participants in these organizations using semi-structured interviews and reviewed their security policy and/or social media policy documents. As this insider
threat is intentional and unintentional in nature (Colwill, 2009; Loch et al., 1992), this study was guided by a theoretical framework that explains intended and unintentioned security behaviour in order to explore this phenomenon. This framework is established from the psychology of security (Pfleeger & Caputo, 2012; Schneier, 2008; Spruit, 1998; West, 2008) and the psychology of intuitive judgement (Kahneman, 2003). The framework steered the design of the interview questions and the findings of our first empirical study.

Five organizations were invited to participate in this study. Four organizations agreed to participate. The participating case organizations and respondents of this study are illustrated Table 1.

<table>
<thead>
<tr>
<th>Case</th>
<th>Pseudonym</th>
<th>Type of Organization</th>
<th>Number of Employees</th>
<th>Informants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>UNI</td>
<td>University</td>
<td>4,000</td>
<td>IT Director, Security Manager, Security Consultant, Security Lecturer</td>
</tr>
<tr>
<td>Case 2</td>
<td>SB</td>
<td>Statutory Body</td>
<td>300</td>
<td>Deputy Director (Security), IT Manager, Security Manager, Social Media Manager</td>
</tr>
<tr>
<td>Case 3</td>
<td>PSU</td>
<td>Public Service Unit</td>
<td>3,000</td>
<td>IT Manager, IT Compliance Manager, Security Manager, Incident Response Manager</td>
</tr>
<tr>
<td>Case 4</td>
<td>SC</td>
<td>Security Company</td>
<td>300</td>
<td>Research Director, Incident Response Director, Security Manager, HR Manager</td>
</tr>
</tbody>
</table>

Table 1. The list of case organizations and participants

Referring to Table 1, the case organizations were chosen because these organizations were dealing with different classifications of organizational information from non-confidential to confidential information and they rely on IS to carry out their business processes. Therefore, it is important for these organizations to protect their valuable information.

With the indication from the literature and reports that the use of social media among employees can cause leakage of organizational information, we needed to understand how and why leakage happened. Therefore, prior to this study, we interviewed 22 employees across the four case organizations. We found that employees were disclosing work-related information to perform tasks and to communicate with their colleagues about meetings, tasks, celebrations, commiserations and frustrations. We incorporated these findings into three hypothetical scenarios and we used different names, positions and job descriptions to preserve the confidentiality of the participants.

In the present study, from 16 to 31 January 2012, we went back to the four organizations, but this time we interviewed 16 security managers to confirm that employees’ OSN behaviour and the types of work-related information that employees disclosed online had the potential to incriminate organizational information security. During the interviews, we showed three hypothetical scenarios of employees’ OSN activities captured from the previous study.

The first scenario presented five Facebook conversations about work that employees, in a hypothetical organization, disclosed online. These conversations were in the form of Facebook status updates that were centred on information about the organization, superiors, work tasks, meetings and colleagues, as shown below:

A. Attention @List_of_Colleagues: Don’t forget our meeting tomorrow at 10am to discuss the launching of the new system. @ZaitonAli and @ShamNizam, don’t forget the slideshow ya? Hope the boss will be in a good mood!

B. Check out the photos taken at the company dinner last night. Took some pics with the boss and also some VIPs! I think the VVIP’s wife was way too overdressed LOL!

C. The stupid reshuffling made me work with Ms E now. As usual, she is taking a 3-day-leave when the deadline is in 3 days! How can I finish the work on time all by myself? HELP!

D. Congrats @SherryShah for the promotion! Hope you can be a better boss than Mr. X!
E. Goodbye @AmanAmin, Company XYZ is lucky to have you! It’s better to work for a company that appreciates you...

Scenario 2 was about a hypothetical organization that restricted the use of social media during working hours. However, employees in this organization were still communicating about work with their colleagues and friends, using applications and playing games through their mobile devices. Some of them even used Facebook to update locations of meetings and their whereabouts (currently, this is equivalent to geotagging capability on social media or the Place or Check In function on Facebook).

Scenario 3 expanded one of the Facebook conversations in Scenario 1 to include comments made by the user’s colleagues. This scenario showed how a post that was innocuous could turn out to be sensitive due to comments made by others.

In each of the scenario, we asked the security managers how these conversations and OSN activities could implicate their organizations, what were their similar experiences, their current security strategies that could address these issues, and their opinions on better strategy that could be implemented. From their responses, we managed to capture various types of security strategies that the organizations implemented and the factors that influenced their strategy decision. We also looked at their security policy and/or social media policy documents to justify some of their answers.

All interviews, which lasted 45 - 60 minutes on average, were audio-recorded and transcribed in verbatim manner for analysis.

4 ANALYSIS

The verbatim transcriptions resulted in 110 pages of text. Hence, data reduction and analytic categorization of data were done on the verbatim transcriptions whereby the data was coded sentence-by-sentence to identify the themes and subthemes. We analysed the data based on thematic analysis technique (Boyatzis, 1998; Lee, Mitchell, & Sablynski, 1999), grounded theory analysis approach (Strauss & Corbin, 1998) and pattern matching (Yin, 2009). Generally, transcribed data was grouped into categories of themes derived from the literature and the ones that emerged from the data. Then, we compared and contrasted the analysed interview data with the descriptive field notes gathered during document reviews. Technically, based on the literature and research trainings on analysis of qualitative data, the data was analysed using the following steps:
- reading and re-reading the transcripts,
- highlighting key statements that reveal attitudes, beliefs, and perceptions of relevance to research objectives,
- coding the key statements into themes and redefining them when new themes emerge,
- using spreadsheets to place key statements according to themes,
- identifying patterns of similarity and difference,
- summarizing the patterns for each case,
- finding meanings from the results based on research aims, and
- drawing cross-case conclusions.

From the analysis, we categorised our findings into these themes and subthemes shown in Table 2.

<table>
<thead>
<tr>
<th>Themes</th>
<th>Subthemes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSN impacts on security</td>
<td>Information leakage</td>
</tr>
<tr>
<td></td>
<td>Information / Intelligence gathering</td>
</tr>
<tr>
<td></td>
<td>Reputation issue (of organization, superiors, colleagues)</td>
</tr>
<tr>
<td></td>
<td>Malware distribution</td>
</tr>
<tr>
<td></td>
<td>Identity theft</td>
</tr>
<tr>
<td></td>
<td>Network bandwidth problem</td>
</tr>
<tr>
<td></td>
<td>Work productivity issue</td>
</tr>
<tr>
<td></td>
<td>Internal conflicts</td>
</tr>
<tr>
<td>OSN security strategy</td>
<td>Authorized OSN access</td>
</tr>
<tr>
<td></td>
<td>OSN security policy</td>
</tr>
</tbody>
</table>
Table 2. Themes and subthemes of the study

5 FINDINGS

This section presents the findings based on the themes shown in Table 2. Due to the limitation of the number of pages for this paper, not all subthemes will be discussed.

5.1 OSN Impacts on Security

Generally, all security managers agreed that all Facebook conversations shown in the hypothetical scenarios had the potential to incriminate organizational information security. Most of them informed that leakage of information was the direct impact of these conversations. A security manager from the Statutory Body (SB) mentioned that, “The number one threat is information leakage. In today’s world, information is more valuable than money. Competitors and enemies are looking forward for such leakage to happen”. Similarly, a security manager from the Security Company (SC) highlighted how such leakage could cause cyber espionage. He cited that, “…people who know about espionage, (would think) all five examples (of Facebook conversations among employees) have values. People put many information on Facebook, …a platform we now call OSINT, Open Source Intelligence”. A security manager from SB asserted the implications of complaining about work on Facebook, “Complaining about work on Facebook is embarrassing to the company and to themselves. It may tarnish the organization’s reputation, the employees also portray themselves as unprofessional”. Interestingly, a security manager from the University (UNI) talked about the difficulty to control employees’ postings on Facebook. He quoted that, “This division has had employees who had resigned because of the things that they were not happy about. It did not stop there because even after their resignation, they still continue to back bite certain people and continue to gossip on Facebook. Since they had left the university it was difficult for us to take action”.

5.2 OSN Security Strategy

Our samples showed a common way of framework in dealing with employees’ use of social media, which involved people, process and technology elements of security strategy. Based on their implemented strategies, we categorized them into authorized OSN access, OSN security policy, OSN security education, training and awareness programs, and OSN security technical control. The implemented strategies are shown in Table 3.

<table>
<thead>
<tr>
<th>Subthemes</th>
<th>Case 1 - UNI</th>
<th>Case 2 – SB</th>
<th>Case 3 - PSU</th>
<th>Case 4 – SC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized OSN access</td>
<td>All employees were given full access to social media without formal controls.</td>
<td>Employees were allowed to use social media but access to games, apps, chats and links was restricted. Only employees who were using social media for work purposes were given full access.</td>
<td>All employees were only allowed to access social media outside office hours (before 8.30am, 1.00pm-2.00pm, after 5.00pm). However, during these times, the use of games and apps was restricted.</td>
<td>All employees were given full access to social media. However, video streaming was only allowed for 15 minutes.</td>
</tr>
</tbody>
</table>
OSN Security Policy

No social media policies. Security policies had been developed but not implemented due to lack of management support. Incidents were handled at departmental level.

In the process of finalizing social media policies. Security policies were developed and implemented but lack of enforcement.

Security policies and social media policies were developed and implemented. However, the enforcement of the policies was still lacking.

Social media and security policies had been developed, implemented and enforced. Employees were not allowed to post information about work on OSN sites except for employees assigned to use the sites for work.

OSN Security Education, Training and Awareness (SETA) (Whitman & Mattord, 2008)

No formal SETA programs. Security and social media seminars and talks were organized by staff and students on ad-hoc basis. Reminders were given to all employees through emails and during meetings when social media incidents happened.

Security trainings were given to new employees during induction. Security trainings were given for employees with security duties. Security awareness talks for all employees were carried out a few times a year.

Security trainings were given to new employees during induction. Security trainings were given for employees with security duties. Security awareness including social media use talks for all employees were carried out 1-2 times a year.

Security trainings were given to new employees during induction. Security certification trainings and exams were set for security employees. Security awareness talks for all employees were held four times a year. Continuous reminders were given during monthly meetings and through emails.

Technical Control

Limit the network bandwidth for social media use during peak periods (student online registration).

Web filtering system to limit social media use among employees.

Web filtering system to limit social media use among employees.

Data leakage prevention (DLP) system to enforce social media policies.

Table 3. Strategies to minimize information leakage through OSN

Based on the OSN security strategies shown above, the depth and sophistication of the implemented strategies increased from Case 1 to Case 4. Case 1 (UNI) had an ad-hoc way of dealing with its employees’ OSN activities. OSN incidents were handled at the departmental level and there was no formal policy with regards to employees’ use of social media. Its security policy had been developed but not yet implemented. Although Case 2 (SB) had no formal policy on OSN, it had informal guidelines for social media use among employees. It also had established comprehensive information security policies, which was quite similar to Case 3. Case 3 (PSU) was viewed to have the strictest control of OSN accessibility and was the first among all four cases to establish the policy on social media. However, both Case 2 and Case 3 faced issues in enforcing their policies and they were both lacking of behavioural control mechanisms. Case 4 (SC) was considered to have the most comprehensive and holistic approach of addressing information security issues posed by employees’ OSN. It covered the integrated approach which included organization, people, process and technology aspects which is similar to the Business Model for Information Security presented by the Information Systems Audit and Control Association (ISACA), an international professional association that deals with governance of information technology (ISACA, 2010). These different levels of depth, integration and sophistication of the implemented strategies across these four cases, motivated us to propose a Maturity Framework for OSN Security Management.
5.3 Factors Influencing OSN Security Decision

The study also found that there were some characteristics that shaped the way the four case organizations employed OSN security strategies. The organizational characteristics somehow influenced the way these organizations decided on the strategies. These characteristics are as follows:

5.3.1 Management perception of security impacts of employees’ OSN

In this study, perception is defined as the process of selection, organization and interpretation of the input from individuals’ senses to give meaning and order to the world around them (George & Jones, 2005). The interviews with security managers from UNI implied that management’s perception of employees’ OSN behaviour was viewed as compartmentalized; organizational, technical and social issues were treated in silos, not integrated as a holistic organizational issue. Some of UNI participants informed that the management would respond to their security incidents’ report only when it was focused on operational related matters, such as employees’ productivity. One of the security managers quoted,

“We have suggested to the management about gaming addiction among employees. We didn’t give the security implications but highlighted the productivity issues instead. Therefore, we could get the buy in from the HR division... They think information security is IT Division’s responsibility and not theirs.”

On the other hand, SC perceived social media use among employees as a holistic organizational information security issue, in line with their mission and vision as the security services provider. Its security managers’ feedback shows employees’ use of social media had impacts on security, business, technical and social concerns. One of them asserted that,

“...you have to weigh the benefits, the pros and cons of doing this (posting work-related information on social media). If the piece of information is very valuable, you can’t afford to lose it, you might as well need to invest on it since relying on people alone is not sufficient, we need people, process and technology.”

5.3.2 Management’s perception of information sensitivity

Our conceptual study indicated that many organizations failed to specify the sensitivity of organizational information based on security perspective. This was similar to our empirical findings whereby in some cases, information was deemed sensitive because it might hurt people’s feelings or affect people’s credibility, rather than it might affect the confidentiality, integrity and availability of information. Some participants mentioned that information about work that was posted on Facebook was sensitive because it might affect the reputation of the boss. While reputation of a superior would reflect the reputation of the organization, to us, it was more of a cultural issue than a security issue. Hence, organizations’ perception of information sensitivity is considered as one of the important criteria to understand organizational information security practices.

5.3.3 Management’s commitment to supporting OSN and security initiatives

In line with the management’s perception of OSN security impacts and of information sensitivity described earlier, these perceptions had an effect on their commitment to supporting OSN security initiatives. According to security managers from UNI, a group of security consultants (internal and external) initiated the development of UNI’s security policy. The security policy document was approved by the management but the policy was yet to be implemented due to lack of management support in terms of assigning responsibilities throughout UNI to implement the policy. One of security managers cited,

“The policy document that we had developed last year was not implemented since we are still waiting for the management’s decision on the (security responsibility) structure. They have approved the document, but have not approved the implementation.”
In accordance to the above, the assignment of OSN security responsibility within an organization also influenced the way organizations implemented their strategies. Organizations could assign this responsibility to a department or individuals. As mentioned in section 5.3.1, management’s perception of security impacts of employees’ OSN behaviour in UNI was viewed as compartmentalized. This finding confirmed that view since UNI relied on IT Department for IT-related matters including information security. However, IT Department received little support from the management in terms implementing information security programs within UNI. According to some security managers, UNI expected users to be responsible for their OSN activities since they were given the freedom to engage in social media. However, when an incident happened, there was no formal control mechanism, it was up to the head of the department or IT department to take action.

6 DISCUSSION AND CONCLUSION

This paper started with some real cases of information leakage through OSN that had made the headlines globally. It was shown that the use of OSN sites among employees had been so pervasive with the advancement of social technologies. The pervasiveness of social media becomes a double-edged sword to organizations; it is beneficial at the same time it could be detrimental. People can access social media at the workplace, at home and while on the go (using mobile devices). This accessibility blurs the boundary of professional and personal communications, allowing inadvertent leakage of organizational information through the public domain. Such leakage provides an opportunity for cyber criminals to do surveillance on employees’ OSN pages and gather intelligence to perform targeted attacks on organizations (Leitch & Warren, 2009; PricewaterhouseCoopers, 2010; Smith & Toppel, 2009). Therefore, organizations need to manage the use of social media among employees while at the same time safeguarding their valuable information from being accessed by unauthorized individuals.

This pervasive phenomenon and the little coverage in academic literature motivated us to study this area. Our findings confirmed that employees were disclosing information about work that might jeopardize organizational information security. Thus, we unravelled different types of security strategies that could mitigate security issues around employees’ OSN. We also captured the factors that influenced the decision that organizations took to implement the security strategies. Across the four case organizations, we found different levels of sophistication of the implemented strategies. Hence, we decided to propose a maturity framework that might be used by organizations to evaluate their capability to address security issues through OSN. Due to the page limit, the framework is not presented in this paper. We are hoping to do so in our upcoming paper.

This research is significant since it addresses the gap concerning the behavioural and organizational aspects of IS security and the gap concerning OSN security impacts on organizations. It is also considered as important and timely due to the current attention given by the media to this contemporary phenomenon.

References


Acknowledgement
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 Computing & Information Systems, The University of Melbourne. Her PhD education is financed by the Malaysian Ministry of Higher Education and the International Islamic University Malaysia.