International Journal of Information Management xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

# A case analysis of securing organisations against information leakage through online social networking

Nurul Nuha Abdul Molok[a], Atif Ahmad[b,*], Shanton Chang[b]

[a] Department of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[b] School of Computing and Information Systems, The University of Melbourne, Victoria, Australia

ARTICLE INFO

*Keywords:*
Information leakage
Information security management
Online social networking
Maturity framework

ABSTRACT

The inadvertent leakage of sensitive information through Online Social Networking (OSN) represents a significant source of security risk to organisations. Leakage of sensitive information such as trade secrets, intellectual property and personal details of employees can result in a loss of competitive advantage, loss of reputation, and erosion of client trust. We present 4 case studies which examine drivers for employee leakage behaviour and corresponding security management strategies. Drawing on these case studies, we present a maturity framework for organisational OSN Leakage Mitigation Capability (OSN-LMC) and lessons learned from the case analysis.

## 1. Introduction

Leakage of sensitive information across organisational boundaries is a significant and increasing security risk for organisations. Sensitive information may include trade secrets, intellectual property, business strategies, product or service related details and even confidential client and customer information. The impact of such leakage can result in a range of organisational impacts including loss of competitive advantage, loss of reputation, loss of revenue, and loss of opportunity especially where clients are sensitive to information breaches (Ahmad, Bosua, & Scheepers, 2014).

Online Social Networking (OSN) is akin to a 'leaky pipe' as the technology is designed such that communications between the sending party and the intended recipients are visible to other parties as well. Leakage through OSN is (1) instantaneous as it is available to the audience immediately upon posting, (2) ubiquitous as it is globally accessible across myriad demographics, and (3) persistent in that is archived in perpetuity (Schneier, 2009). These characteristics entice end-users to engage with OSN but they also create opportunities for information leakage (Cascavilla, Conti, Schwartz, & Yahav, 2017). We define information leakage as "*a breach of the confidentiality of information, typically originating from staff inside an organisation and usually resulting in internal information being disclosed…*" across organisational boundaries (ISF, 2007, p.2).

A review of the literatures of Information Security Management (ISM) and OSN shows that although considerable research has focused on the intersection between these 2 discipline areas, relatively less research has looked at the strategies of security managers aimed at mitigating the risk of OSN leakage. We therefore ask the following research question:

How can organisations mitigate the risk of sensitive information leakage via OSN?

We begin this paper with a focused review of literature on security risks of OSN and relevant security management controls. Subsequently, we describe the research methodology, develop a maturity framework and present lessons learned.

## 2. Risks and strategies in information leakage through OSN

Sensitive organisational information is exposed to risks as employees embrace social media as part of their lives. Employees' OSN activities such as accepting friends' requests, posting organisational information, using third party applications and playing games, have the potential to contribute to information leakage. Table 1 illustrates the key functionalities of OSN sites and related leakage risks to organisations.

The ISM literature suggests that mitigating security risks such as OSN leakage requires a comprehensive range of security measures including formal controls (e.g. information security policy and risk management), informal controls (e.g. security education, training and awareness) and technological controls (e.g. firewalls and VPNs) as a means of maintaining a security environment (Ahmad et al., 2014).

* Corresponding author.
*E-mail addresses:* nurulnuha@iium.edu.my (N.N. Abdul Molok), atif@unimelb.edu.au (A. Ahmad), shanton.chang@unimelb.edu.au (S. Chang).

https://doi.org/10.1016/j.ijinfomgt.2018.08.013
Received 24 August 2018; Received in revised form 26 August 2018; Accepted 27 August 2018

**Table 1**
OSN functions and potential risks (adapted from Abdul Molok, Ahmad, & Chang, 2012).

| OSN Functions | Potential Security Risks | Potential Impacts to Organisations |
|---|---|---|
| Post information / update status | Users may inadvertently disclose sensitive information through OSN posts/ updates as access to OSN is by anyone, anywhere, anytime, using any devices | Unauthorized access or deduction of information of value from inadvertent disclosures |
| Friend Requests | Carelessness in accepting friend requests increases risk of adding untrusted users | Monitoring of organisational targets and social engineering attacks to progress an impending attack |
| Upload photos and videos | Photo albums and videos may inadvertently disclose sensitive information | Photos and videos may contain sensitive information resulting in a range of impacts |
| Third party applications and links to external sites | Third party content may contain malware or links that enable inadvertent disclosure | Use of compromised client platforms to further an impending attack |

However, the literature does not address how these can be coordinated in an OSN strategy to address the specific challenge of leakage.

## 3. Case study method, selection and background

We conducted a multiple case study to examine common patterns in firms where OSN leakage is a security risk and because cross-case analysis allows for greater insight into the phenomenon as well as stronger validation of the empirical data. Our decision to study four organisations was based on the fact that maturity frameworks need at least three to four levels to be useful and multiple case study research in ISM (and more broadly in Information Systems research) has previously reported on anywhere between two and six organisations (Eisenhardt, 1989). The specific choice of case organisation was determined from the level of leakage risk posed to the organisation.

We reviewed the literatures in ISM and OSN to identify leakage risks specific to OSN (a brief summary of the review is presented in Section 2, leakage risks are in Table 1). To acquire an appreciation of the security management challenges of OSN leakage, we investigated the perspectives of employees and security managers (see Table 2). Interviews were used as the primary data collection instrument, while participant observations and document reviews were secondary sources of research data (Yin, 2017).

The four in-depth case studies were conducted in Malaysia. The data collection included observations, document reviews and interviews of 38 respondents examining (1) the drivers of the OSN leakage phenomenon in terms of leakage behaviour among employees, and (2) measures taken by security management to mitigate the risk of leakage. Case study data collection occurred in two phases. In the first phase, we interviewed employees and followed them on Facebook, and collected/ determined (1) online communication with colleagues, (2) disclosure of work-related information and (3) factors that influenced information leakage. Based on these findings, we prepared two sets of anonymized scenarios of perceived risky OSN activities. In the second phase, we went back to the four case organisations to confirm the scenarios represented real risks and we interviewed security managers to determine: (1) OSN impacts on organisational information security, (2) factors influencing information leakage through OSN and (3) managerial attitudes (perception and commitment) that influenced strategy decisions.

Drawing on the case study results, we developed the OSN Leakage Mitigation Capability framework (OSN-LMC). The aim of the proposed maturity framework is to assess an organisation's capability to mitigate the risk of sensitive information leakage via OSN. A related aim is to provide guidelines for organisations to improve their current capability. The maturity framework functions as a self-assessment tool to evaluate and/or improve the organisational capability or maturity to mitigate leakage impact. The audience or users of the proposed framework are strategic security management responsible for managing organisational information security.

The case selection was opportunistic in nature, as we already had established trust relationships with these public and private organisations. Trust was critical to gaining the necessary access because of the sensitive nature of the topic and because organisational policy and strategy documents pertaining to information security are often considered confidential in organisations. Table 2 illustrates the case organisations and respondents.

Our analysis showed that the 4 case organisations existed at different levels of maturity in relation to the security management of OSN. The results from the case studies were highly useful in refining the scope of the maturity framework and framing the security management challenges around security perception of employees, security management practices and also resources that are related to mitigating the leakage of information via OSN. The rich data from the 4 cases helped to define the criteria and provide examples for how the criteria might work in practice.

Compared to staff at the other case organisations, employees at UNI were the least aware of leakage risk when discussing work and performing tasks on OSN. Interestingly, we also found a low-level of information security readiness with UNI's security management. Security incidents on social media were handled at the departmental level on an ad-hoc basis and there was no formal policy addressing social media use in the organisation or resources assigned to dealing with the governance of OSN.

Employees at SB reported that there were technological controls on social media. They could access Facebook at work, however access to external links, games, and applications was restricted. Unlike UNI, where employees openly discussed work on their status updates, most employees at SB used group forums and private messages for the same purpose. Some showed an understanding of OSN implications to security, however there were reports of risky behaviour such as locations of meetings were disclosed, and mobile devices were used to play

**Table 2**
The list of case organisations and participants.

| Case # /name | Employees | Employee Interviewees | Security Management Interviewees |
|---|---|---|---|
| 1 / University (UNI) | 4,000 | IT Lecturer, Secretary, IT Assistant, Account Assistant, Personal Assistants (2). (3 males, 3 females) | IT Director, Security Manager, Security Consultant, Security Lecturer (4 males) |
| 2 / Statutory_ Body (SB) | 300 | System Analyst, Secretary, IT Assistant, Personal Assistants, Administrative Assistant (4 Females, 1 Male) | Deputy Director (Security), IT Manager, Security Manager, Social Media Manager (3 males, 1 female) |
| 3 / Public_ Service_ Org (PSO) | 3,000 | IS Officer, Project Officer, IT Assistant, Administrative Executive, Secretary (4 Females, 1 Male) | IT Manager, IT Compliance Manager, Security Manager, Incident Response Manager (2 males, 2 females) |
| 4 / Security_Firm (SF) | 300 | Development Executive, Executive Secretary, Secretary, Multimedia Executive, Security Analyst, Media Executive (4 Females, 2 Males) | Research Director, Incident Response Director, Security Manager, HR Manager (4 males) |