Implications of Social Media Networks on Information Security Risks

Literature review

James Boorman, Yanhua Liu, Yixin Zhang, Yu Bai, Siyi Yao, Mengxue Wang and Li Tai

Abstract

The user base of Social Media Networks (SMN) has grown dramatically over the last 10 years, with the Facebook platform alone commanding 18% of the world’s population as active users. Thus SMN provide a mechanism to disseminate information both rapidly and globally. Despite this fact, little research has been conducted into the implications of SMN on information security risk. Here we conduct a literature review in order to provide information security professionals with insight into the threats, threat agents, vulnerabilities and potential risks faced by individuals and organisations from SMN. Findings suggest that confidentiality and integrity of information can be threatened by multiple actors and mechanisms, putting information and reputation at risk. Information security professionals face a mammoth task to manage such risks and a standard approach to risk management seems unlikely to be effective.

Introduction

The terms Online Social Networks (OSNs; Park et al 2014) and Social Networking Sites (SNS; Young & Quan-Haase 2013) are used to describe social networking services such as Facebook. Here we adopt Kane et al’s (2014) terminology of “Social Media Networks” (SMN) to describe Facebook and other services where users:

“(1) have a unique user profile that is constructed by the user, by members of their network, and by the platform; (2) access digital content through, and protect it from, various search mechanisms provided by the platform; (3) can articulate a list of other users with whom they have a relational connection; and (4) view and traverse their connections and those made by others on the platform.”(Kane et al 2014, p279).

The use of SMN has grown rapidly, Facebook’s user base has grown to 1.28 Billion active users since launching in 2004 (Facebook 2014), approximately 18% of the world’s population (United States Census Bureau 2014). This is significant when we consider that the population figures include infants and those who either cannot use, or do not have access to a computer. Thus SMN enable rapid global exchange of information, potentially exposing users to a number of information security risks (Squicciarini et al 2011; Ahmadinejad & Fong 2014).

Information security risk management is a process focused on the preservation of the confidentiality, integrity and availability of information (Webb et al 2014). In order to protect information, organisations must first identify what information they have, assess its value and potential risks through the risk assessment process (Shedden et al 2010). The effectiveness of risk management standards and risk assessments in practice for the identification and protection of information assets has been debated (Vidalis et al 2004; Siponen 2006; Parker 2007; Shedden 2010; Shedden 2011; Webb 2014). Suggested critical success factors include: establishing the context of the assessment to accurately reflect the organisations objectives and goals; involving a large number of stakeholders in the process; and adopting a continuous improvement approach to identify existing and emerging assets, threats, vulnerabilities and validate the effectiveness of controls (Vidalis 2004; Spears & Barki 2010).

As Kane et al (2014) note, many organisations are only just starting to utilise SMN, thus little is known about the potential impact to the organisation. Here we conduct a review of the literature of SMN in order to answer the question:

What are the implications of Social Media Networks on Information Security Risks?
Literature Review

The body of knowledge from A* and A ranked journals on the information security risks posed by SMN is limited (see table 1) and focused on the confidentiality of personal information. It is noted that studies have used relatively small samples sizes when compared to the user base, with a lack of longitudinal data and a Western cultural bias. Thus the findings may not be representative of the wider user population or emerging trends.

Privacy vs. function - the loss of confidentiality

When signing up to a SMN service, users are required to create a personal profile that contains various pieces of personal information, such as: full name; date of birth; email address; and photo (Young & Quan-Haase 2013). Such information is of value as it can be used to conduct identity theft and/or used in attacks to overcome authentication measures in online services for financial gain (Tow et al 2010; Ahmadinejad & Fong 2014). Although there is no specific requirement or mechanism to verify the accuracy of this information in order to gain access to SMN services, many users chose to accept the risk and disclose accurate information in their profile (Young & Quan-Haase 2013). Alarmingly, not all users are aware of the need to protect this information or how to use the various privacy controls offered by SMN platforms (Tow et al 2010; Young & Quan-Haase 2013).

Given the vast potential audience for information disclosed on SMN, the probability of personal or sensitive information being misused is high, yet users continue to disclose personal information in profiles, wall posts and updates (Chen & Sharma 2013). Chen & Sharma (2013) suggest that SMN drives disclosure by providing a community that encourages others to share, building trust and encouraging further self-disclosure. This information can then be accessed by the SMN provider or other parties in order to develop targeted marketing campaigns (Chen & Sharma 2013). Interestingly many users are willing to ignore such privacy risks if SMN services provide functionality that is perceived as useful (Tan et al 2012; Xu et al 2013). A side effect of the photo tagging feature in Facebook, is the damage that can be done to the confidentiality of private events. Uploaded images are subject to the privacy settings of the user who uploaded the image, thus you can be tagged and identified on Facebook irrespective of having an account or not (Squicciarini et al 2011). Even if you do have an account, you no longer have control over how your image is used and who may have access to it. Tagged images are searchable and the SMN service maintains ownership of the image (Squicciarini et al 2011), further limiting an individual’s control.

Rumours - the loss of integrity

The role of SMN users in contributing to breaking news stories from their mobile devices has been well documented, yet the quality and accuracy of the information provided remains dubious (Oh et al 2011; Doer et al 2012; Oh et al 2013). The pervasive nature of SMN and the ease of mobile access, provides multiple unverified sources of information that may rapidly degrade the integrity of the original information and generate inaccurate rumours (Oh et al 2013). Further, given the global interconnected nature of SMN, rumours spread fast, far and wide. Mathematical modelling from Doer et al (2012) suggests that 80% (45.6 Million at the time of publication) of Twitter users can receive a rumour “within only eight rounds of communication” (Doer et al 2012, p71). 

Threats, threat agents and vulnerabilities

Despite the reported use of privacy controls, the confidentiality of information stored on SMN is not guaranteed. The identity of friends is uncertain, with profile cloning enabling impersonation and the easy creation of fake identities, used to tempt or trick users into disclosing valuable personal information (Jin et al 2013; Park et al 2014; Ahmadinejad & Fong 2014). Even if friends are known, the dissemination of Information may be rapidly amplified by unintentional or intentional re-sharing, with further dissemination subject to their network of friends and each individual’s privacy settings (Kleinberg, 2008; Kane et al 2014). Further, Jin et al (2013) demonstrate that information can be discovered and inferred on Facebook and LinkedIn via mutual friend connections outside a user’s direct friend group.

Young & Quan-Haase (2013) report that although many users make use of privacy settings to control disclosure amongst their Facebook friends, they are less concerned about extending such controls to
third-party applications. This is a worrying trend given that additional functionality often comes from third-party web applications. These applications are hosted on servers outside the control of the SMN provider, managed by unknown people and with unknown levels of protection and no guarantee that the information collected will be protected or used lawfully (Ahmadinejad & Fong 2014). The situation doesn’t get better, with Scholte et al (2012) reporting that the complexity of successful attacks against web applications hasn’t changed significantly, with similar vulnerabilities continuing to be exploited in new and existing applications despite awareness campaigns for software developers. Further, exploitable vulnerabilities often exist upon release of an application and may exist for many years before being resolved (Scholte et al 2012). An example of this issue comes for the release of the Diaspora SMN service. Diaspora is aimed at improving privacy as a backlash against Facebook, but vulnerabilities in the release put the confidentiality of user’s information at risk (McKenzie 2011).

Putting the application vulnerabilities to one side, Ahmadinejad & Fong (2014) report varying success from attacks using a third-party application on Facebook to infer the content of confidential information, using information that is publicly available within and outside the SMN. As Ahmadinejad & Fong (2014) point out, even with a low yield of success when using their single simplistic algorithm, given the massive user base, such attacks may damage the confidentiality of information from a large number of users.

Methodology

The University of Melbourne Library Discovery search was used in order to find literature in the field of SMN. Search terms were selected by the authors and results filtered for A* and A ranked journals as determined by ACPHIS (2014). Results were further refined during literature review workshops. A summary of search results in shown in in table 1.

<table>
<thead>
<tr>
<th>Search term</th>
<th>Filtered result (number of articles returned)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online social networks</td>
<td>2,274</td>
</tr>
<tr>
<td>Online social networks risk</td>
<td>24</td>
</tr>
<tr>
<td>Online social networks attack</td>
<td>14</td>
</tr>
<tr>
<td>Online social networks security</td>
<td>39</td>
</tr>
<tr>
<td>Online social networks social engineering</td>
<td>48</td>
</tr>
<tr>
<td>Online social networks source of intelligence</td>
<td>9</td>
</tr>
<tr>
<td>Social network sites risk</td>
<td>9</td>
</tr>
<tr>
<td>Social network sites attack</td>
<td>9</td>
</tr>
<tr>
<td>Social network sites security</td>
<td>31</td>
</tr>
<tr>
<td>Social network sites social engineering</td>
<td>24</td>
</tr>
<tr>
<td>Social network sites source of intelligence</td>
<td>3</td>
</tr>
<tr>
<td>Social network sites information security risk</td>
<td>7</td>
</tr>
<tr>
<td>Social media security</td>
<td>19</td>
</tr>
<tr>
<td>Confidentiality integrity availability online social network</td>
<td>0</td>
</tr>
<tr>
<td>Unintended disclosure of information</td>
<td>3</td>
</tr>
</tbody>
</table>
Discussion

Here we apply the identified threats, threat agents and vulnerabilities form the literature review to explore potential risks to organisation information security posed by SMN services.

The scope of the problem

The risks posed by SMN to the confidentiality and integrity of information are immense. SMN are now part of everyday life, they can be accessed from any number of devices at any time. The confidentiality and integrity of information posted on SMN is affected by many factors outside of an individual’s or organisation’s control. Anyone can pretend to be anyone they like and post anything they want (irrespective of accuracy) from any device to a global audience at any time. Re-dispersal of information is dependent on: vulnerabilities in the platform and third-party applications; multiple privacy settings; and the intentions of anyone who receives the information (Kleinberg, 2008; Oh et al 2011; McKenzie 2011; Doer et al 2012; Scholte et al 2012; Oh et al 2013; Young & Quan-Haase 2013; Kane et al 2014). Adding to this, SMN platforms have a symbiotic relationship with their user base as they are seen to benefit from encouraging disclosure, with users more likely to continue to disclose more information when provided with perceived functional benefits (Tan et al 2012; Xu et al 2013).

Examples of the loss confidentiality

One of the most infamous examples of the loss of confidentiality of information due to unwitting disclosure via SMN, involved the wife of the head of the British Secret Intelligence Service (MI6). Here information about Sir John Sawers was published on his wife’s Facebook account and available to all users due to a lack of privacy controls (BBC 2009). The information disclosed included: an identifying photo of Sir John; information about and the location of “their children”, “their flat” and his parents; “transport arrangements”; and connections with “senior diplomats” (BBC 2009). It is assumed that the information disclosed was not Top Secret, although its disclosure may have had national security implications and posed direct risks to the confidentiality and availability of information for MI6. Risks could include: kidnap and interrogation; surveillance and interception; or assassination. It is assumed that numerous security controls, training and a mature risk assessment process were in place, however MI6 failed to protect this information outside their organisation.

A more disturbing example of the uncontrolled disclosure of sensitive information via SMN from individuals outside an organisation, comes from the Mumbai terrorist attacks (Oh et al 2011). These tragic events unfolded rapidly and were covered in detail by civilians on the ground using Twitter (Oh et al 2011). Where in the past authorities would be able to control what information was disclosed in the media in order to protect active operations, this time they had no control over the rapid and global disclosure of information via Twitter (Oh et al 2011). Tweets included the disclosure of sensitive information regarding the Indian Government activities in response to the terrorist actions, which were duly monitored by the terrorist commanders and relayed to the terrorists conducting the attack (Oh et al 2011).

The risk of commercial disclosure

The opportunities for discovering and disclosing commercial information may be obvious. Anyone who comes into contact with commercial conversations, documents or electronic information can be considered a threat agent. For example, conversations, documents and information displayed on screens and whiteboards can be recorded on any mobile device or discussed either knowingly or unwittingly on SMN. Once this information has been disclosed on SMN, the organisation has lost control and thus the confidentiality of the information.

The less obvious risk comes from social engineering, where people obtain information by deception. For social engineers, SMN are a potential gold mine of information. Mitnick & Simon (2002) describe the stages of a social engineering attack. Here we note that these stages can now be provided quite easily with SMN, without the need to dive through rubbish bins, dress up as tradesmen or conduct cold calling. The first stage involves gathering background information on a chosen target in order to establish a ‘pretext’ for the attack (Mitnick & Simon 2002). This can now quite easily be conducted via a Google or Facebook search, commonly returning a wealth of information. If this fails, then an attacker can choose to clone a
profile, explore a mutual friend or inference attack (Jin et al. 2013; Ahmadinejad & Fong 2014). Next, the attacker makes use of the information gathered in order to develop ‘rapport and trust’ (Mitnick & Simon 2002, p329). The SMN platform assists the attacker, by providing the community that encourages trust and the disclosure of information (Chen & Sharma 2013), accepting the attacker into our network of friends. In the next stage, having established a ‘rapport’, the attacker exploits our feelings of trust, manipulating us into disclosing sensitive information. Again the sense of community created by the SMN platform assists the attacker here and especially so if our ‘friend’ is recommending this new ‘killer’ third-party application (Tan et al. 2012; Xu et al. 2013; Ahmadinejad & Fong 2014). Finally the attacker uses the information gathered, such as our date of birth and inferred answers to security questions to bypass authentication measures and access our bank account or organisation’s systems (Ahmadinejad & Fong 2014).

Even if the new ‘killer’ feature isn’t provided by a malicious group or unscrupulous competitor and the information is handled in the strictest of confidence, without being on sold to others, ownership and control of the information has passed outside the organization. The confidentiality of this information may still be subject to attack via unknown vulnerabilities in the web application (Scholte et al. 2012) or from inference attacks (Jin et al. 2013; Ahmadinejad & Fong 2014).

The problem doesn’t stop at the employee, as demonstrated in the example of Sir John Sawers. Simple onward disclose can come from the re-posting of information by any SMN connection in the employees group of SMN friends, with further amplification subject to each individuals privacy settings (Kleinberg, 2008; Kane et al. 2014). Further, the same vulnerability or inference attacks can then be carried out against any of these connections (Jin et al. 2013; Ahmadinejad & Fong 2014). Intelligence gathering via profile cloning and mutual friend based attacks may further enrich the level of detail inferred or encourage disclosure via deception (Jin et al. 2013; Park et al. 2014; Ahmadinejad & Fong 2014). Information obtained may be used to attack authentication mechanisms, which often use similar security questions and answer responses, potentially exposing access to the organisation or an individual’s bank account (Ahmadinejad & Fong 2014).

Outside of the systems realm, we hypothesise that the level of such information gathered over time may be useful to competitors to infer sensitive information. For example: revealing the identity of team members; the progress on a particular project inferred by the hours worked; the morale of key team members and opportunities to affect the availability of information and tacit knowledge by poaching talent; and to inform surveillance operations to obtain richer information for espionage or blackmail. Additionally, we hypothesise that profile cloning may be used to damage the integrity of information. Here misinformation may be fed to a project team by impersonating a team member, friend, customer or key stakeholder.

The challenge of integrity and the risk to reputation

Despite employees being careful with what they disclose, organisations still face the problem that the accuracy of information provided by users on SMN can be dubious (Oh et al. 2011; Doer et al. 2012; Oh et al. 2013). This may be further complicated by the fact that the identity of users is uncertain (Jin et al. 2013; Park et al. 2014; Ahmadinejad & Fong 2014). Threat agents may be unscrupulous competitors, malicious ‘trolls’ or disgruntled employees posting feedback from supposed customers, or posting ‘official’ information while impersonating employees on any SMN platform outside the control of the organisation. Even if all posts are genuine, the reputation of an organisation can be rapidly damaged given the speed at which rumours can be generated and their global reach (Doer et al. 2012). Oh et al. (2013) note the reputational damage suffered by Toyota from the global exposure of its recall programme that was widely discussed on SMN.

Conclusion

Organisations and individuals face risks to the confidentiality and integrity of information stored in and provided by SMN services. Raising awareness of the complexity of potential threats, threat agents and vulnerability may assist in identifying potential risk. However, information security professionals face a mammoth task in developing effective controls to reduce these risks. Given the variety of potential sources and the velocity of global dissemination via SMN, a standard approach to risk management seems unlikely to be effective.
References


Author/s:
Boorman, James; Liu, Yanhua; Zhang, Yixin; Bai, Yu; Yao, Siyi; Wang, Mengxue; Tai, Li

Title:
Implications of social media networks on information security risks

Date:
2014-08

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/42192

File Description:
Implications of social media networks on information security risks