Securing organizations against information leakage through Online Social Networking: Case analysis and maturity framework

Nurul Nuha Abdul Molok, Atif Ahmad, Shanton Chang
nurul.nuha@iium.edu.my[1], atif@unimelb.edu.au[2], shanton.chang@unimelb.edu.au[2]
[1]Department of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]School of Computing and Information Systems, The University of Melbourne, Australia

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 examining drivers for employee leakage behaviour and corresponding security management strategies addressing OSN leakage. Drawing on these case studies, we present a maturity framework for organisational OSN Leakage Mitigation Capability (OSN-LMC) and lessons learned from the case studies.

Keywords: Information Leakage, Information Security Management, Online Social Networking, Maturity Framework

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 organizational 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 is 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 organizational information is exposed to risks as employees embrace social media as part of their lives. Employees' OSN activities such as accepting friends' requests, posting organizational information, using third party applications and playing games, have the potential to contribute to information leakage. In fact, even if strict privacy and security settings have been set, sensitive information on targeted employees can still be gathered through their profiles (Külcü & Henkoğlu, 2014). Table 1 shows key functionalities of OSN sites and the related leakage risks to organizations.

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, it is 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 organizational 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

Table 1: OSN functions and potential risks (adapted from Abdul Molok et al., 2012)

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). 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. 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 this security 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 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 (see Table 2).

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)

Table 2: The list of case organisations and participants

Our analysis showed that the 4 cases 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 games. In our interactions with SB, security managers showed a comprehensive understanding of the potential security impacts of employees' OSN.

At PSO there were reports of employees who: (1) revealed the location of a confidential meeting, (2) posted photos about the launching of a new system, and (3) downloaded a Facebook proxy to bypass network restriction. In fact, some respondents admitted that they had brought their own laptops and other mobile devices to access social media at work. However, there was no evidence that respondents were using Facebook to perform tasks. Access to social media was restricted during office hours but there was no attempt at explaining to employees why this was important. The security experts indicated that there was difficulty in enforcing security policy and social media policy beyond the technology controls. Although the IT Security Division was responsible to implement OSN security strategies in PSO, the responsibility was also given to each departmental head to ensure employees adhered to the policies.

Employees at SF indicated that there was a policy on posting organisational information on social media. However, one of the respondents did show OSN behaviour that seemed risky such as competing with colleagues in Facebook games and posting information about the boss on her status update. Nevertheless, we found that SF employees exhibited a better understanding of acceptable security behaviour around OSN. Employees were very aware of security strategy on social media use and they provided a thorough understanding of security risks of employees' use of social media compared to the other case organisations. The security experts frequently spoke about information security covering the confidentiality, integrity and availability of organisational information. The security governance around social media was also the most comprehensive among the 4 cases. SF covered an integrated approach of OSN security strategy, which involved organisation, people, process and technology domains.

4. The Online Social Networking – Leakage Mitigation Capability Framework

We identified seven independent factors from the case study evidence that collectively represent the capability of an organisation to mitigate OSN leakage. The first five relate to security management practices. These were 1) Integration of OSN policy and security policy; (2) Security Education, Training and Awareness (SETA); (3) Technology Control on OSN; (4) OSN Security Responsibility; and (5) Management commitment to support OSN security initiatives. The last two relate to critical perceptions that influence said practices. These were: (6) Management perception of OSN Security Impacts; and (7) Employee awareness of OSN security. We developed these areas into precise self-audit questions to assist organisations to assess their maturity.

There were sufficient distinguishing features across the seven criteria to have 4 different levels of maturity. These different capabilities were mapped as Level 1 'Reactive' (low capability due to ad hoc strategies), Level 2 'Planned' (medium-low capability due to strategies being planned but not implemented), Level 3 'Managed' (medium-high capability due to strategies addressing OSN and

security being structured), and Level 4 'Integrated' (high capability due to sophisticated security strategy, governance and control around social media). The lower levels have a more *fragmented* approach to OSN strategy as they have relatively isolated strategies at those levels. The higher levels are considered to have a more *holistic* or integrated strategy approach.

Formulating the 7 factors into self-audit questions for security managers allowed us to identify evidence from each of the case studies that could form the basis of maturity criteria. We were careful to ensure that the maturity framework as a whole had discriminatory power in the sense that the criteria could be used to distinguish between levels of good practice. Table 3 outlines the maturity levels and representative quotes from participants of our multiple-case studies that were used to structure and evidence the maturity criteria and attributes.

	Level 1: Reactive OSN Security Capability	**Level 2: Planned OSN Security Capability**	**Level 3: Managed OSN Security Capability**	**Level 4: Integrated OSN Security Capability**
Criterion 1 Management perception of OSN Security Impacts	*"We have suggested to the management about (Facebook) gaming addiction among employees, but we didn't give the security implications but highlighted the productivity issues instead. Therefore, we could get the buy in from the management"* (Security Manager)	*"When I was managing a large team, the staff didn't give their cooperation, (and) talk bad things behind my back. So just imagine if they talk about these on Facebook, your reputation is at stake, people will judge you"* (IT Manager)	*"…it is better to restrict the staff from using social media during office hours. However, they can use the media after 5pm. But if you think that Facebook is a tool that is dangerous to the organization, can tarnish the reputation, maybe you should consider banning the site completely"* (Security Manager)	*"…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 process, people and technology."* (Incident Response Director)
Criterion 2 Management commitment to support OSN security initiatives	*"...the security team has already brought up these issues, but it is difficult to get the management buy in. The policy document that we had developed last year was not implemented since we are still waiting for the management's decision"* (Security Manager)	*"We need to provide the understanding not only to the operational level employees but most importantly the top management level... If they understand the importance of security and give their commitment, then only we can implement security within the organizations"* (Security Manager)	*"We received tasks from top level management to monitor Facebook, usually regarding identity theft and information leakage" (*Security Manager)	*"…we have monthly meetings with the CEO, he always reminds everyone (about security)… During security management committee meetings, where all the HODs are there, the reminder is cascaded down to the employees"* (Research Director)
Criterion 3 OSN Security Responsibility	*"Each user should be responsible to understand the privacy and security settings on Facebook. To rely on us (IT Division) to monitor the postings is just too much, there are too many (postings) to monitor*	*"They (the management) think information security is IT Division's responsibility and not theirs."* (Security Manager)	*"Each department is responsible to educate their staff; the immediate superior is responsible to give one-to-one advice to subordinates who are disclosing inappropriate things about work on FB"*	*"The management must think how to overcome and minimize the problem. It has to be cascaded down to the last employees. …Any problem about social media must be discussed... Whatever the outcome of the discussion must be*

	and we don't have the resources to do that" (Security Manager)		(IT Compliance Manager)	*communicated to the staff"* (Research Director)
Criterion 4 Employee Awareness of OSN Security	*"Privacy settings? I have never used it… Does this mean everyone can see my photos?"* (Secretary)	*"…I am not aware (about OSN security issues) … But I did read in the newspaper about stolen identities on Facebook, it can pose some dangers to people"* (Admin. Assistant)	*"When users expose too much information about the organization, it might affect the organization's reputation. Playing games and links can open doors to malware threats"* (IS Officer)	*"In my personal opinion you should not be posting about your work. It draws a lot of attention from others… whatever information that you post and whatever photos that you upload, there is a risk behind it"* (Executive Secretary)
Criterion 5 OSN Security Policy	*"So far there are no written policies on the use of social media among employees but whenever there was an incident, the employees are being reminded about the proper use of social media."* (IT Director)	*"...enforcement of the policies must be done by the organization. Incidents had happened, but employees were just being warned, no other action was taken (according to the policies)"* (Security Manager)	*"We need to increase the enforcement, …to make sure that information security become the priority"* (Incident Response Manager)	*"We have a social media policy that states official information is not allowed to be posted on these sites, except for the employees who manage the official pages."* (Security Manager)
Criterion 6 Security Education, Training and Awareness	*"I have not seen (security) programs within the past 8 months since I joined the company"* (Security Manager)	*"In terms of awareness, we regularly arrange talks from the industry and employees are all invited to attend the (social media security) talks"* (Security Manager)	*"When new employees come in, they are given induction training for 1 week which includes a topic in information security"* (IT Compliance Manager)	*"We have done awareness programs to explain the policy to them. …every quarter of the year. We also have security quizzes, treasure hunts and other fun things in order to educate the staff about security."*(HR Manager)
Criterion 7 Technical Control of OSN	*"We limit the network bandwidth primarily because of (network) performance issues"* (IT Director)	*"…we limit the access to games, apps, chats and links. (To do this) We used a web filtering system to control the access based on individual use."* (IT Manager)	*"We also have content filtering system that can filter any unauthorized sites and contents"* (Incident Response Manager)	*"In some instances, for you to enforce something, you have to use technology…like DLP to protect your information"* (Incidents Response Director)

Table 3: Maturity criteria, levels and quotes from case study participants

The OSN-LMC framework (Figure 1) is a practical management instrument that can be used: (1) to focus a range of security measures including security policy, SETA, and technological controls on the leakage mitigation problem, and (2) as a rapid audit tool to assess existing leakage mitigation capability. However its true potential is realized when used as an improvement tool in a transformational process from 'reactive' to 'integrated' OSN security management.

	LEVEL 1 – REACTIVE OSN SECURITY MANAGEMENT	LEVEL 2 – PLANNED OSN SECURITY MANAGEMENT	LEVEL 3 – MANAGED OSN SECURITY MANAGEMENT	LEVEL 4 – INTEGRATED OSN SECURITY MANAGEMENT
What is management's perception of the possible security impacts of employees' OSN?	• Employees' OSN is perceived to have no impact on the organization	• Employees' OSN is perceived to have an impact on productivity	• Employees' OSN is perceived to pose security risks to the availability of corporate technology infrastructure	• Employees' OSN is perceived to pose a wide range of security risks including technology availability as well as information confidentiality and integrity
What evidence is there of management's level of commitment to OSN security strategy?	• Managerial response is ad hoc, triggered by OSN security incidents. There is a lack of governance structures around OSN security such as OSN Security Policy for longer-term support	• Evidence of low level commitment from management. Management provides little support for the implementation of OSN security strategy	• Evidence of medium level commitment from management. Management supports the implementation of OSN security strategy	• Evidence of high level commitment from management in the shape of dedicated budget, policy review, mandatory reporting, etc. Management provides clear direction and support for OSN security strategy
Has responsibility for OSN security been clearly assigned?	• Responsibility has not been formally assigned to an entity. Employees are assumed to be responsible for their own OSN activities	• OSN security has been generally assigned to a department (for e.g. IT Department)	• OSN security has been assigned to high level management. For e.g. HODs are generally responsible to ensure policy compliance among employees	• OSN security responsibility has been assigned to a unit that consists of security specialists and reps from various business functions. Shared OSN security culture exists; OSN security responsibility is shared amongst employees
To what extent are the employees aware of the possible security implications of their OSN behaviour?	• Employees are unaware of the security implications of their OSN behaviour • Evidence of widespread risky behaviour	• Low level of awareness of the security implications of OSN behaviour • Evidence of occasional risky behaviour	• Medium level of awareness of the security implications of OSN behaviour • Evidence of infrequent risky behaviour	• High level of awareness of the security implications of OSN behaviour. • Risky OSN behaviour rarely happens
What is the level of OSN policy integration with overall security policy? To what extent is OSN security policy enforced?	• Neither formal OSN policy nor security policy exists • Response to problems is ad hoc	• Low level of integration • OSN policy and security policy are implemented but not clearly documented	• Medium level of integration • OSN policy is integrated with security policy, are both implemented but neither are clearly enforced	• High level of integration • OSN policy is Integrated with security policy, are both implemented, clearly enforced and adapted to the changing threat landscape
How comprehensive are OSN security training and education programs?	• No formal OSN security education exists • OSN security training is ad hoc	• OSN security training is compulsory for newly inducted employees • Neither ongoing training nor education exists	• OSN security training is compulsory for newly inducted employees • A refresher training is offered periodically	• OSN security trainings are conducted periodically for all employees • Ongoing OSN security education for professional development is given to employees who are responsible for OSN security management
How sophisticated is technical security control around OSN use?	• No technical security controls are applied directly or indirectly to control OSN over a long term, however some controls may be applied temporarily after incidents take place	• Network resources are constrained to indirectly control OSN (e.g. bandwidth limitation)	• Custom control targeted to OSN are used (e.g. web filtering controls)	• OSN is controlled using mechanisms that integrate web, apps and data (e.g. web filtering, data leakage & integrated access management systems)

Figure 1: Online Social Networking – Leakage Mitigation Capability (OSN-LMC) Framework

5. Lessons Learned

The case studies revealed an organizational conflict in values emerging as a result of increased adoption of OSN technologies on the one hand and concerns about the disclosure of sensitive information on the other. The conflict arises from the situated use of OSN symbolizing a different set of values to the end-user group than the security management group. Many employees in the case organizations felt they had no choice but to use social media to contact colleagues and supervisors about work-related issues (which increased the risk of disclosure of sensitive information) as they would not respond to email in a timely manner. Whereas security managers were of the opinion that employees used social media because they were addicted to the technology and ignorant of the security impacts. This conflict presents a significant obstacle for organizational learning as security managers must recognize the causes of security risks, if security controls (e.g. policy, training) are to effect changes to OSN behaviour (Ahmad, Maynard & Shanks, 2015).

We learned that OSN security measures were strongly influenced by management perception of the impact of OSN security risks. All the respondents perceived that employee OSN activity had significant implications for organisational information security. However, most of the organizations employed OSN security strategies for reasons other than leakage mitigation, such as the negative affect on employee productivity (UNI, PSO) and/or a supervisor's credibility (UNI, SB, PSO), and disruption to technology availability (SB). Only SF perceived social media use among employees as a holistic security issue in line with their mission and vision as a security services provider.

We found a clear link between management perception of OSN security impacts and their commitment to supporting OSN through assignment of security responsibilities and resourcing security initiatives. In terms of the former, SF had the most comprehensive approach. The responsibility to handle OSN leakage was delegated to the Security Management department (which also developed and implemented the security policy) with support from SF's steering committee. Clear lines of responsibility existed with representatives from the Security Management department assigned to the departments in SF. A separate social media policy was developed and implemented by the Corporate Communications department. This approach contrasts with UNI, where the responsibility to manage OSN leakage was delegated to the general IT function with no top management support, and no formal process for handling incidents. The other two organizations delegated the responsibility to develop security policy to the security and/or IT function but enforcement was left to the various heads of each department.

In terms of supporting OSN security initiatives, in one of the respondents (UNI), management approved the security policy document but the policy was yet to be implemented due to lack of management support in assigning responsibilities to carry out the plan. A similar situation applied to two of the other respondents (SB and PSO). Even when leaks would occur, management would not take disciplinary action as stipulated in the policy. However, in contrast with the other three, SF's more holistic view of information security translated into formal and frequent reminders from top management to employees about the importance of protecting organisational information. Further, our review of SF's security and social media policy documents and responses from respondents showed clear enforcement of both policies (security policies and social media policies).

A surprising lesson we learned was that some security managers were less concerned about the security risk of disclosure to the organisation, and more concerned about the impact to the reputation of senior managers. This phenomenon can be explained by the fact our case studies were conducted in Malaysian organisations and that Malaysia's power distance index ranks amongst the highest in the world (Hofstede, 2017). In countries where the status difference is so pronounced, our case studies suggest there is a greater likelihood that managers will not understand the motivations behind employee actions. This was certainly observed in some of the organisations with low levels of maturity.

6. Conclusion

The case study research explores how and why the use of social media by employees can result in inadvertent leakage of sensitive organizational information. It provides rich insight from both employees and management about this pervasive phenomenon, which is affecting organizations globally. The paper presents a maturity framework that can be used by security practitioners as a self-assessment tool to evaluate an organisation's as-is situation to mitigate leakage risk. The framework also provides the progression of an OSN security strategy that can be used by security researchers for further research. The framework may be employed by security practitioners to guide and/or to improve the mitigation of OSN security issues in organisations.

7. References

Abdul Molok, N. N., Ahmad, A. and Chang, S. (2012) 'Online social networking: a source of intelligence for advanced persistent threats', *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 2(1), pp. 1–3.

Ahmad, A., Bosua, R. and Scheepers, R. (2014) 'Protecting organizational competitive advantage: a knowledge leakage perpective', *Computers & Security*, 42, pp. 27–39.

Ahmad, A., Maynard, S.B., & Shanks, G. (2015). A Case Analysis of Information Systems and Security Incident Responses. *International Journal of Information Management*. 35(6), (pp. 717 - 723).

Cascavilla, G., Conti, M., Schwartz, D. G., & Yahav, I. (2017). The insider on the outside: a novel system for the detection of information leakers in social networks. *European Journal of Information Systems*, 1-16.

Eisenhardt, K. M. (1989) 'Building theories from case studies research', *Academy of Management Review*, 14(4), pp. 532–550.

Hofstede, G. (2017) *What about Malaysia?* https://geert-hofstede.com/malaysia.html Accessed 9 April 2017.

ISF (2007) *Information Leakage*, *Information Security Forum Briefing No.4*. Information Security Forum. http://www.securityforum.org. Accessed 5 May 2010.

Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. International Journal of Information Management, 34(6), 761-769.

Schneier, B. (2009) *A Taxonomy of Social Networking Data*, *Schneier on Security.* http://www.schneier.com/blog/archives/2009/11/a_taxonomy_of_s.html Accessed 10 March 2010.

Yin, R. K. (2017) *Case Study Research and Applications: Design and Methods*. 6th edn. California, USA: SAGE Publications, Inc.