Issues in Information Systems
Volume 17, Issue IV, pp. 109-119, 2016

GRADUATE STUDENT PERCEPTIONS OF PERSONAL SOCIAL MEDIA RISK: A COMPARISON STUDY

Samuel H. Goh, Northern Kentucky University, samuel.goh@nku.edu
Paul M. Di Gangi, University of Alabama at Birmingham, pdigangi@uab.edu
Julio C. Rivera, University of Alabama at Birmingham, jrivera@uab.edu
James L. Worrell, University of Alabama at Birmingham, worrellj@uab.edu

ABSTRACT

Social media usage continues to grow at an exponential rate. The academy is beginning to understand not just the potential, but also the risks involved. This paper compares the results of a Delphi study using a graduate student panel to a prior study using an undergraduate panel. Our results provide a well-rounded, rank-ordered list of the important risks that serves as a jumping point for class discussions in cyber security-related curriculum.

Keywords: Social Media, Risk Assessment, Personal Social Media Risk, Delphi Study

INTRODUCTION

> *Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work.*
> *~ Prospective Job Applicant*
>
> *Who is the hiring manager? I'm sure they would love to know that you will hate the work. We here at Cisco are versed in the web.*
> *~ Tim Levad, Channel Partner Advocate – Cisco Systems*

One hundred and forty characters and it was gone. In the middle of an economic recession, a job offer extended to a prospective employee from a well-respected technology firm would normally be seen as a positive opportunity for both parties. One hundred and forty characters later; a lesson in the intimacy created among social media users that traverse the World Wide Web is learned. A survey of Alexa.com, a leading web analytics company, shows eight of the ten most visited sites in the world are social media sites (e.g., Facebook #1 and YouTube #3). Social media is a relatively new phenomenon that can be defined as "*a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0 and that allow the creation and exchange of user generated content*" (Kaplan & Haenlein, 2010).

When social media is enhanced by mobile technologies, users are even more interconnected and are able to share richer content. For example, popular social media updates like FourSquare check-ins that include location data and tagged Facebook photos let users share with others their experiences in a more personal and richer manner. Yet, the constant stream of geo-located shared information could have both potentially positive and negative impacts. One extreme example would be the website PleaseRobMe.com which aggregated twitter feeds and check-ins posts on Foursquare into a live stream, in order to highlight the dangers of making others aware of when a user was not home and oversharing.

These examples highlight the need for a better understanding of the risks associated with personal social media usage. Building on a prior study that explores the perceptions of undergraduate students (Rivera et al., 2015), this paper conducts a Delphi study with graduate students that may view personal social media risks in a more nuanced form to include their personal and professional lives. The results of this study are compared against the results of

Rivera and colleagues (2015). This paper provides a well-rounded, rank-ordered list of the important risks that could serve as a jumping point for class discussions in cyber security-related curriculum.

LITERATURE REVIEW

A review of the literature on the risks of social media usage suggests that studies describing social media risks fall into two primary areas: social risk and technology-based risk. A short discussion of each area and tabular summary is provided in Appendix I.

Social Risks

The bulk of the literature thus far concentrates on identifying the social risks of social media usage at an individual level with relatively fewer papers that address organizational risks. Some risks identified for individual social media use included a loss of productivity (van Zyl, 2009), cyber bullying (Krasnova et al., 2009), cyber stalking (Hogben, 2007), identity theft (Krasnova et al., 2009), or even social information overload (Boyd, 2008). From a professional career standpoint, risks include inconsistent personal branding (Kane et al., 2009), being viewed as a laggard in adoption of social media (Lowell et al., 2009), damage to personal reputation (Argenti & Druckenbiller, 2004; Aula, 2010; Boyd, 2008), and security risks associated with leaked data (Boyd, 2008; van Zyl, 2009). Other authors note that once something is posted online and is stored or indexed, it becomes difficult to control and the data can be used for unintended commercial purposes (Krasnova et al., 2009)

Technology-based Risks

Risks that are specific to the social media technology platform include malicious software (i.e. malware), hacks, and unauthorized access to social media accounts (Hogben, 2007) and service interruptions (Rivera et al., 2015). Service interruptions are especially crucial, given that many companies have come to depend on frontline customer support live via Twitter. Social media account hacks have become nearly too commonplace with barely a footnote in the daily news, but making social media more mobile-friendly has come at a security cost. Other technology-based risks highlight the dynamic and ungoverned nature of social media, such as unreliable user-generated content (Di Gangi & Wasko, 2009; Di Gangi et al., 2010), intentional or unintentional violation of legal requirements (Kane et al., 2009), and a distorted view of the market due to a vocal and visible minority (Helm & Jones, 2010).

METHODOLOGY

A multi-panel Delphi approach was used to understand social media risks from an individual perspective. As the focus of the study is to identify salient social media risks perceived by graduate students, a Delphi study which enables the rank-ordering of risks are, is well-suited to addressing this question.

Delphi Methodology

The Delphi technique is analytic method developed by the RAND corporation in the 1950s (Worrell et al., 2013). It is a process that incorporates quantitative and qualitative measures and feedback in multiple steps. The main purpose is to take responses about important issues from an expert panel and to further refine those responses into a rank-ordered list of issues that is derived from group consensus (Delbecq et al., 1975). The first step in a Delphi study is normally to identify the relevant issues. The issues may be brainstormed by the participants themselves, seeded (provided to the panel by the researchers), or a combination of both.

Based on the initial list of issues, the panelists independently rank order the issues from most to least important. The responses are collected anonymously, in order to reduce the chance of group think or bias. Along with the rank order, each panel member is asked to provide qualitative feedback justifying the relative rank. After the responses are collected, a non-parametric statistic that assesses the degree of consensus of the rankings for the entire panel, Kendall's W, is computed. Similar to a correlation, a Kendall's W score ranges from 0 to 1, where 0 represents no consensus and 1 represents complete consensus. The qualitative feedback and Kendall's W score is relayed back to

the panel, constituting the end of a round. Subsequent rounds where the panel is asked to re-rank the items based on the feedback and degree of consensus from the prior round continues until at least a moderate degree of consensus (Kendall's W score of > 0.6) is achieved or decreases as a result of panel exhaustion (Worrell et al., 2013).

To identify the key risk factors associated with social media and the importance of these risks, this study duplicated the Delphi study of Rivera and colleagues (2015) using graduate students in a large, public southeastern university. Graduate students were enrolled in a special topics course on social media and virtual communities. The graduate student group was composed of individuals with professional work experience in the education, energy, finance, healthcare, insurance, and technology sectors. By comparing these Delphi results with those of Rivera and colleagues (2015), this study broadens the sampling frame demographics and enhance the generalizability of the results. Further, a comparison of the rankings between groups reveals other meaningful insights.

Expert Panel Selection and Composition

The graduate student panel included 29 students enrolled in a special topics course focused on the strategic impact of social media on business processes and outcomes. The panel was composed of 12 males and 17 females with 69% between the ages of 18 and 29. For comparison purposes, Rivera and colleagues (2015) conducted a study with 22 undergraduate students composed of 13 male and 9 female students enrolled in a junior-level business course at a small, rural southern university in the United States.

Social Media Risk Seeding

The graduate student panel was provided with a comprehensive list of risks associated with social media based on the risks identified in the literature review section. The panelists were asked to first identify which the important risks were by identifying the top ten. Rankings were not collected during this process as the initial step was to narrow down the list into a more manageable size. Risks which were identified by more than 50% of the panelists, for each panel, were then used in the ranking rounds.

Data Collection and Analysis Method

Panelists rank-ordered the randomized, seeded list provided by the researchers. Between rounds, the average ranking for each item, Kendall's W statistic, and standard deviations were computed. Qualitative feedback, as provided, was collected to justify the ranking of the items. This data was provided as feedback for the next round of the Delphi. The Delphi continued till the conditions to terminate were satisfied (e.g. a moderate consensus to strong consensus was reached or panel fatigue).

RESULTS

Overall, 22 risks were identified by the graduate and undergraduate student panels and 15 risks overlapped between the panels. This suggests a general consistency amongst panel members of the key risks facing individuals as a result of the use of social media. Figure 1 depicts the Kendall's W statistics for both Rivera and colleagues (2015) and the graduate student panel conducted in this study. When comparing the graduate panel against the undergraduate panel, the graduate student panel indicated a slightly stronger degree of consensus of the risks facing personal social media use.

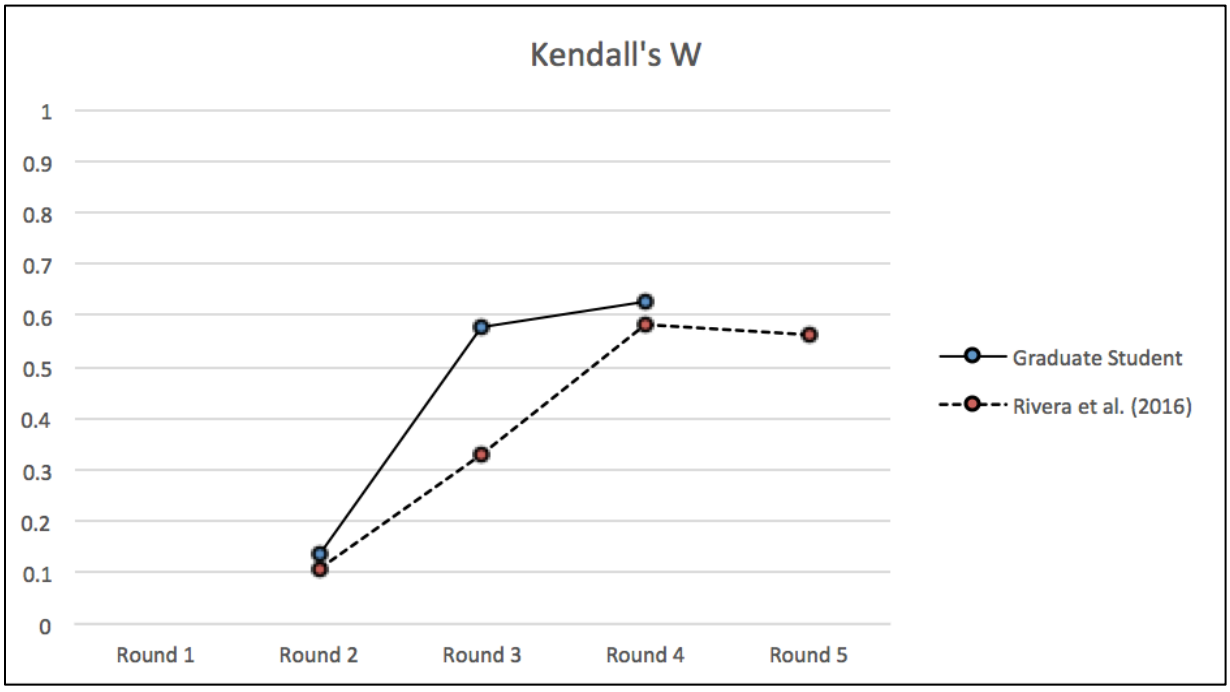

Figure 1. Delphi Kendall's W Results

Both panels assessed social media risk as it applies to individuals in terms of personal or professional implications (i.e., risk to the individual when using social media). Starting with the organizationally-oriented panel and concluding with the individually-oriented panel, these results are presented below.

Graduate Student Panel Results

For the graduate student panel, individual risks were reduced to 10 risks. Kendall's W for the third ranking round was 0.626, which indicates moderately strong agreement in the rankings among the panelists (Schmidt, 1997). Based on feedback from the panelists and guidance from previous Delphi studies (Worrell et al., 2013), it was determined that a significant drop off in panelist participation would occur had a fourth round been requested; therefore, the Delphi study was discontinued. Table 1 presents the results of the graduate student panel ordered by rank and showing the average rank of each risk in each Delphi ranking round based on panelist responses. Round 1 is not included in the table because it was used to narrow the number of risks to a manageable set and not for ranking purposes.

Table 1. Graduate Student Delphi Panel Results

Individual Risk Perceptions		**Average Rank by Delphi Round**		
Rank	**Round**	**2**	**3**	**4**
1	Online content may be used for identity theft	3.440	1.770	1.560
2	Malicious software/malware	4.520	2.810	2.840
3	Source of information for hackers/social engineering	4.590	3.650	3.640
4	Hacks / unauthorized access to social media account	5.110	4.960	4.400
5	Damage to personal reputation	5.190	5.040	5.040
6	Cyber-stalking	5.890	5.960	6.400

7	Online content shared with unintended third parties for commercial purposes	6.300	6.770	7.000
8	Decreased personal productivity	6.560	7.040	7.040
9	Cyber-bullying	6.700	8.040	8.160
10	Uncontrollable actions	6.700	8.960	8.920
	Kendall's W	***0.134***	***0.578***	***0.626***

The risks associated with social media were perceived social risks with technical risks being somewhat important in specific circumstances. Primarily, graduate student panelists were concerned social media profiles would be used for social engineering and identity theft attacks (Online content may be used for identity theft (1st) and Source of information for hackers/social engineering (3rd)). One panelist argued that identity theft could be a higher order risk where Damage to reputation (5th), Decreased productivity (8th), and Unauthorized access to resources (4th) are potential consequences to identity theft:

> *"To me, identity theft is the biggest threat of the use of social media because it can impact so many areas of your life. It is many of these things rolled into one- it can damage reputation, decrease productivity (b/c it is a lot of work to get straightened out and it is on your mind a lot), and it is gaining unauthorized access to personal resources."*

Such an argument can logically include Cyber-bullying (9th) and Cyber-stalking (6th) as social media presence creates opportunities for criminals to monitor and engage in negative actions towards an individual all of which can be seen as Uncontrollable actions (10th) to a victim. In contrast to the social risks which dominate the overall risk rankings, technical risks were seen as important as well. The second largest risk from social media was the potential for Malicious software/malware (2nd) where an individual clicks on a malicious link or installs malicious software due to the use of social media and Hacks/Unauthorized access to social media account (4th). Taken collectively, the graduate student panel indicates that both social and technical risks are important with both being represented in the top two risk perceptions. However, social risk represents a larger share of the overall risk perceived by graduate students when using social media.

Undergraduate Student Panel Results Comparison

For the undergraduate student panel, Rivera and colleagues (2015) resulted in 11 identified risks. Kendall's W reached a peak consensus of moderate agreement in the third round (W = 0.585), with the consensus dipping in the subsequent round (Kendall's W = 0.562) (Schmidt, 1997). Due to a peak being experienced, Rivera and colleagues (2015) concluded that no further rounds were necessary. Table 2 compares the final Delphi results of the graduate student panel against Rivera and colleagues (2015) undergraduate student panel results.

Table 2. Personal Social Media Risk Perceptions

Rank	Risk	Graduate Student Panel Final Avg Rank	Rivera et al. (2015) Final Avg Rank	Graduate Panel Final Rank	Rivera et al. (2015) Final Rank
1	Online content may be used for identity theft	1.560	2.17	1	1
2	Malicious software/malware	2.840	8.28	2	9
3	Source of information for hackers/social engineering	3.640	4.28	3	3
4	Hacks / unauthorized access to social media account	4.400	3.11	4	2

5	Damage to reputation	5.040	4.50	5	4
6	Cyber-stalking	6.400	5.17	6	5
7	Online content shared with unintended third parties for commercial purposes	7.000	9.28	7	10
8	Decreased productivity	7.040		8	
9	Cyber-bullying	8.160	7.17	9	8
10	Uncontrollable actions	8.920		10	
11	Unintended exposure of information		5.61		6
12	Online content may facilitate discriminatory hiring practices		6.56		7
13	Online content may be stored or indexed		9.89		11
	Kendall's W	***0.626***	***0.562***		

Undergraduate student panelists were also concerned that social media profiles would be used for social engineering and identity theft attacks (Online content may be used for identity theft (1st) and Source of information for hackers/social engineering (3rd)), earning identical rank positions as the graduate student panel. An undergraduate student panelist also suggested identity theft could lead to other risks (e.g., Damage to reputation (4th), Unintended exposure of information (6th)) as consequences:

> *"I found identity theft to be the most important risk factor in online social media. Because it has control to take over your identity, steal your assets, and damage your reputation. Identity theft has become a very severe threat to using the internet, and needs to be a risk factor that is handled and stopped."* (Rivera et al., 2015, p. 52)

Interestingly, the undergraduate student panel also identified technical risk as a serious concern when using social media. The second largest risk from social media was the potential for Hacks/Unauthorized access to social media accounts (2nd) where an individual's password is manipulated to obtain access to a personal account. While technical, the risk of Malicious software/malware (9th) was not seen as important to the undergraduate student panel as it was to the organizationally-oriented, graduate student panel. This could be because graduate student panelists took a more structured, holistic approach to not only social media's usage, but also its implementation considerations and interactions with technology devices or systems. In contrast, the undergraduate student panel may not view the risks of social media beyond the relational aspect that is dominant from use. Similar to the graduate student panel, the undergraduate student panel found that social media content could be shared with unintended third parties for commercial purposes (10th) (7th by graduate student panel) as a risk which may be tied to the how social media is Stored and indexed (11th).

Undergraduate student panelists identified a potential legal risk believing that social media use may lead to Online content being used for discriminatory hiring practices (7th). Undergraduate student panelists may feel less aware of privacy settings and techniques for protecting one's personal information. Taken collectively, undergraduate student panel identified a diverse set of potential individual-level risks due to the use of social media including a dominant amount of social risks, some technical risks, and a single legal risk.

DISCUSSION

The purpose of this study was to enhance understanding of the nature of risk inherit in social media for personal use. The comparison to a prior study using undergraduate students offers a more nuanced view of the risk to using social media by individuals. Based on the results shown in Table 2, both graduate and undergraduate students agree that the highest ranked risk was "*Online content may be used for identity theft*". Although both groups ranked this as their highest perceived risk, the average rank calculated for this risk shows more agreement among graduate students (Average Rank 1.560) than it does for undergraduate students (Average Rank 2.17). Similarly, this divergence in average ranking was observed in the other item (*Source of information for hackers/social engineering*), which both groups ranked as third in their perceptions of personal social media risks. A wider divergence was noted in perceptions between the groups. The undergraduate student panel showed less agreement among panelists (Kendall's W = 0.562) than did the graduate student panel (Kendall's W = 0.626). The undergraduate student panel also identified risks that the graduate group did not consider.

The comparison results show that there are differences in personal social media risk perceptions between graduate and undergraduate students. The reasons for this difference in perceptions may lie in several areas. First, the graduate students in this study all had varying amounts of work experience, as well as being enrolled in a course covering social media and virtual communities. The undergraduate students, in contrast, did not have the work experience or the benefit of participating in a class covering social media. While the undergraduate students reported familiarity with social media, the added attention placed on social media by a special topics course may have caused the graduate student panel to further reflect on the inherent risks associated with its use. The graduate student panel identified the risk of personal social media risk decreasing productivity which suggests the possession of work experience perhaps makes them more in tune with the negative impact social media may have on professional responsibilities.

Second, it is possible a generational gap exists between the graduate and undergraduate student panels. Approximately 86.4% of the undergraduate students in the Rivera and colleagues (2015) study were between the ages of 18 and 27 while this study has approximately 69% of its panel between these ages. The 17.4% difference may have swayed consensus more towards individuals that have not "*grown up digital*" and perhaps evaluate technology differently than those that have "*grown up digital*". Research on the different perspectives digital immigrants and digital natives take towards understanding a technology suggest such a perspective may be important to consider as new generations enter the workforce that are accustomed to personal social media use.

Both the similarities and differences in rankings also offer insights for educators. For similarities, the comparison of the two studies found that both panels agreed on several risks that should be considered "*hot topics*" for cyber security classes. Topics such as identity theft, hacking of social media accounts, using posted information against users, and reputational effects dominate the top five risks identified. Better educating students on safeguards such as identity and fraud protection, using multiple-factor authentication, and virus or intrusion monitoring is needed. However, technical safeguards should not be the only point of emphasis as social media, to put it bluntly, has social impacts. For example, an under-addressed topic in the classroom is an ethical discussion on the effects of social media use, especially in the realm of cyber bullying and cyber stalking, and being more circumspect in social media usage.

In assessing the differences between the two panels, several trends were identified. For undergraduate students, the risks identified tended to be more personal in nature. This panel placed a large emphasis on how social media information could be used against them. More specifically, the panel was concerned with how social media posts could have unintended consequences because of inadvertent exposure or that content would be stored or indexed permanently. These characteristics of the openness of social media could then lead to discriminatory hiring practices. This skew towards self-interest could be explained by recency bias and over exposure to sensational media, or it could be a characteristic of the demographic group. A goal of this study was to broaden the scope of inquiry to include graduate students. Comparing these results against the results of our graduate student panel, we found the graduate student perceptions were more nuanced in terms of being inclusive of more technical and managerial risks. These results suggest that educators should move past merely emphasizing "do's and don'ts on social media" and could concentrate more on how social media usage is intertwined with security on a technical

level, and also on personal management of technology devices, social media platforms, and integration aspects of these topics.

Furthermore, the results of these studies provide an opportunity for information security instructors to bridge the gap between personal and organizational social media risk. By focusing on the personal risk aspects of social media, an instructor can introduce students to organizational social media policies and discuss the differences between personal social media risk and organizational risks to using social media. This will result in a more informed workforce and a student aware of personal and organizational implications to using social media.

LIMITATIONS AND CONCLUSION

This study uses a limited sample of subjects enrolled in a single graduate course on social media to discuss the risks of social media usage. While the sample represents an ideal demographic of social media users, caution should be given to the generalizability of these results. As we have demonstrated in this study, the choice of participants can have a biasing effect on results. Including graduate students revealed other nuances of the risks of personal social media usage that were enlightening. Future research should consider duplicating the Delphi panel among a more diverse range of panelists, including C-suite executives, HR managers, information security professionals, and non-traditional workers (i.e., entrepreneurs and e-lance workers) to determine whether the risks identified range in importance dependent upon the context of the individual and her functional background or purpose for using social media.

The adoption of social media has been extremely quick. The academy is just beginning to understand not just the potential, but also the risks involved. This study helps further our understanding of which the important risks are for educators to address in the classroom by identifying and rank ordering the key risks to personal social media use.

REFERENCES

Argenti, P. A., & Druckenbiller, B. (2004). Reputation and the corporate brand. *Corporate Reputation Review*, *6*(4), 368-374.

Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy & Leadership*, *38*(6), 43-49.

Boyd, D. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. Convergence: *The International Journal of Research into New Media Technologies*, *14*(1), 13-20.

Delbecq, A., Van de Ven, A., & Gustafson, D. (1975). Group techniques for program planning: A guide to nominal group and delphi processes. Glenview, IL: Scott, Foresman, and Company.

Di Gangi, P. M., & Wasko, M. (2009). Steal my idea! User innovation community influence on organizational adoption of user innovations: A case study of Dell IdeaStorm. *Decision Support Systems*, *48*, 303-312.

Di Gangi, P. M., Wasko, M., & Hooker, R. E. (2010). Getting customers' ideas to work for you: Learning from Dell how to succeed with online user innovation communities. *MIS Quarterly Executive*, *9*(4), 213-228.

Helm, C., & Jones, R. (2010). Brand governance: The new agenda in brand management. *Brand Management*, *17*(8), 545-547.

Hogben, G. (2007). Security issues and recommendations for online social networks. ENISA position paper (1).

Kane, G. C., Fichman, R. G., Gallaugher, J., & Glaser, J. (2009). Community relations 2.0. *Harvard Business Review*, November.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), 59-68. doi: 10.1016/j.bushor.2009.09.003

Krasnova, H., Günther, O., Spiekermann, S., & Koreleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society, 2,* 39-63.

Rivera, J. C., Di Gangi, P. M., Worrell, J. L., Thompson, S. C., & Johnston, A. C. (2015). Undergraduate student perceptions of personal social media risk. *Information Security Education Journal, 2*(2), 49-56.

Schmidt, R. (1997). Managing delphi surveys using nonparametric statistical techniques. *Decision Sciences*, *28(*3), 763-774.

van Zyl, A. S. (2009). The impact of social networking 2.0 on organizations. *The Electronic Library, 27*, 906-918.

Worrell, J. L., Di Gangi, P. M., & Bush, A. A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems*, 14(3), 193-208. doi: http://dx.doi.org/10.1016/j.accinf.2012.03.003

Appendix I
Social Media Risk Items, Definitions, Literature Source

Item	Definition	Literature Source
Minority Influence or amplification of events	Creation of a distorted sense of market opinion by increasing the visibility of a vocal and visible minority.	Helm & Jones, 2010
Unintended exposure of information	Accidental transmission and disclosure of information to an unintended third party.	Boyd, 2008; van Zyl, 2009
Convergence of personal and professional network	Integration of one's personal and professional life through digital connections, relationships, software applications, etc.	Boyd, 2008
Source of information for hackers/ social engineering	The use of information found on a social media platform to gain unauthorized access to personal resources.	van Zyl, 2009
Decreased personal productivity	Reduction in efficiency and/or effectiveness due to social media usage for social or non-work purposes.	van Zyl, 2009
Unreliable user-generated content	Creation of content (posts, images, etc.) by users which contains misinformation, errors, or other incorrect data.	Di Gangi & Wasko, 2009; Di Gangi et al., 2010; Kane et al., 2009; van Zyl, 2009
Damage to personal reputation	Use of social media in a manner that diminishes how an individual is perceived by others.	Argenti & Druckenbiller, 2004; Aula, 2010; Boyd, 2008; Krasnova et al., 2009; van Zyl, 2009
Uncontrollable actions	Social media content that is shared or contributed about an individual or organization in a manner that is not under the individual's direct control.	van Zyl, 2009
Cyber-bullying	Purposeful acts of harm, which can take the form of harassment, offensive behavior, secret sharing, public embarrassment and humiliation.	Krasnova et al., 2009
Cyber-stalking (stealth stalking)	Use of social media by an individual to engage in the act of voyeurism to monitor the actions of another individual without their knowledge or explicit consent.	Hogben, 2007
Online content may be stored or indexed	Property of social media posts and content that they can be easily searched and/or stored for future access or retrieval by an individual or organization.	Krasnova et al., 2009
Online content shared with unintended third parties for commercial purposes	Use or transmission of an individual's content to a third party for an expected economic gain.	Krasnova et al., 2009
Online content shared with unintended third parties for non-commercial purposes	Use or transmission of an individual's content to a third party for reasons other than economic gain.	Krasnova et al., 2009
Online content may be used for identity theft	Use of information found on a social media platform to impersonate someone else for fraudulent purposes.	Krasnova et al., 2009

Social information overload	Experience of being overwhelmed by the volume of social network information that is presented too quickly to comprehend or absorb effectively.	Boyd, 2008
Perception of social media acceptance/adoption	Concern that an individual may not be adept or savvy at using social media.	Lowell et al., 2010
Inconsistent personal branding	Image of an individual as portrayed via social media may be inconsistent with the image communicated through more traditional means.	Kane et al., 2009
Online content may facilitate discriminatory hiring practices	Use of social media content that is typically deemed inappropriate, unethical, or illegal for the purposes of making hiring decisions or resource assignments.	Rivera et al., 2015
Intentional or unintentional violation of legal or regulatory requirements	Inappropriate sharing of personal or professional information that is deemed confidential or privileged by government laws or other regulatory bodies.	Kane et al., 2009
Service interruption	Temporary inability to access social media applications or platforms.	Rivera et al., 2015
Malicious software (malware)	Use of fake profiles, postings, blogs or other social media content to secretly install malicious software on a person's computer without their consent.	Hogben, 2007
Hacks / unauthorized access to social media account	Unauthorized use of an individual's social media accounts by a third party with the intent to cause harm.	Hogben, 2007