Undergraduate Student Perceptions of Personal Social Media Risk

Julio C. Rivera [1], Paul M. Di Gangi [1], James L. Worrell [2], Samuel C. Thompson [1], Allen C. Johnston [1]
Management Information Systems
[1] Quantitative Methods Department
[2] Accounting & Finance Department
The University of Alabama at Birmingham
Birmingham
AL 35294, USA
jrivera@uab.edu

ABSTRACT: *This article describes a study designed to collect student perceptions of personal social media risks. The study used the Delphi method to rank the risks of using social media as perceived by undergraduate students. The students' rankings were compared to the personal risks of using social media identified and ranked by a group of Library and Information Science professionals. Although there is some agreement in these risk perceptions, there are also considerable differences. The findings suggest it is important to educate all students about the actual risks they face in using social media. For students specializing in information security, it suggests that additional emphasis should be placed on learning about human behavior and social engineering.*

Keywords: Social media, Risk, Student Perceptions, Pedagogy, Delphi, Undergraduate Education

Received: 18 June 2015, Revised 25 July 2015, Accepted 3 August 2015

1. Introduction

Social media has blossomed over the last decade into a ubiquitous phenomenon widely adopted around the world. Social media is commonly 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* (*p.* 61)" [1]. According to Alexa.com, a leading market research and web analytics firm, seven of the ten most frequently visited sites in the United States are categorized as social media. Over 74% of adults in the United States use at least one form of social media [2], 52% of whom use more than one social media site [3]. In the 18 to 29 year old age range typically associated with students enrolled in undergraduate education, 89% of this population use social media [2].

As adoption of social media has increased, so too have news stories and anecdotes showcasing the pitfalls experienced from using social media. Ranging from cyber-bullying to the disclosure of embarrassing information, this student population understands that there are risks to revealing information through the use of social media. For instance, one young teen learned the consequences of publicly tweeting her displeasure about a new job. "*Ew I start this f*** a** job tomorrow*," quickly went

viral on Twitter attracting the franchise owner of Jet's Pizza to summarily fire the teen [4]. While stories similar to this are growing in frequency, pedagogical research has yet to examine how to best assess a student's understanding of the range of personal social media risks they are subject to and educate students on how their personal social media profiles affect their professional standing.

In light of this underserved area of study, the purpose of this paper is to gain an understanding of the personal risks that undergraduate students perceive in their use of social media and consider the pedagogical implications for information security and general higher education programs. The next section briefly highlights the literature on social media and the potential risks of its use. The manuscript then describes the research methodology employed to capture undergraduate student perceptions based on this review and draw comparisons to improve pedagogical practice.

2. Background

The social media landscape is rapidly evolving with new forms of social media, while older forms change to accommodate user and business requirements. This evolution brings with it new ways to collect and share personal information, often without considering the risks to revealing personally harmful information. The demographic distribution of social media users is weighed heavily towards the younger population, including a large cohort of teens, many of whom who will soon be attending college. Social media platforms have also evolved from personal computers to mobile devices including tablets and smart phones. This proliferation of platforms and wide-scale adoption encourage social media users to share information constantly and with little thought to personal risks.

Currently, 87% of adults in the Untied Stated use the Internet [5]. In the 18 to 29 year old age range, 89% of internet users use at least one form of social media [2]. Of the 13 to 19 year old age group, 92% of those online use at least one form of social media [6]. Widespread access to smartphones has also facilitated the adoption of social media and its use. In the teen demographic, 24% report that use social media almost constantly [6], with 56% saying that they use it several times a day [6]. Social media is an integral part of the lifestyle of college bound students.

Social media use is not without risk. The very purpose of social media is to facilitate social relationships and shared experiences through sharing personal information with others to form an online community. Although such sharing might seem innocuous, under certain circumstances it could result in revealing information that harms the individual. The consequences of harmful use of the information shared may be tangible or intangible. Users of social media, whether consciously or unconsciously, assume a certain level of risk when they participate in social media. Tangible risks may include discrimination, identity theft, abuse of power by the state, or physical harm. Intangible risks may include chilling effects, feeling helpless, or apprehension of future harm [7].

A recent study sought to develop and rank a list of personal risks incurred by social media users. This study created a taxonomy of personal risks and organized them into the categories described above [7]. Using this taxonomy, a group of Library and Information Science professionals developed a ranked list of personal risks associated with the use of social media. Table 1 outlines these risks in ranked order. Although this is a list developed by experts in the area, it may not reflect the risks that undergraduate social media users perceive.

Given these findings, academics must consider how they prepare current and future college students to deal with the personal risks involved in using social media. News coverage has made everyone aware of some of the dangers of revealing personal information through social media, but most news stories sacrifice measured and helpful coverage in the interest of sensational headlines. As a result it is fair to assume that most social media users have a distorted view of the personal risk associated with using social media. This study offers a glimpse of how undergraduate students perceive the personal risk of using social media. It also provides recommendations for addressing social media risks through pedagogy.

3. Methodology

To capture student perceptions of social media risk, this study employed the Delphi method. The RAND Corporation developed the Delphi method in the early 1950's [8]. Although there are various ways of implementing a Delphi study, the implementations

Item	Score	Overall Rank
Identity Theft	1,934	1
Strangers able to see sensitive personal details	1,841	2
Targeting by advertisers	1,575	3
Victim of fraud	1,531	4
Discrimination by employer or potential employer	1,443	5
Targeting by criminals (e.g. sharing that you are away from home, thereby welcoming burglars.)	1,411	6
Friends, family or colleagues able to see sensitive personal details	1,297	7
Cyber-bullying or harassment (including stalking)	1,288	8
Targeting by official bodies or security agencies	980	9
Extortion or blackmail	628	10
Prosecution by authorities due to crime allegations	590	11
Physical violence or kidnapping	451	12

Table 1.Ranking or Risks from a Survey of LIS Professionals [7]

generally share four characteristics. First, a panel of participants in the area to be studied is convened and works anonymously.

The panelists either brainstorm on a pre-defined topic or comment on a pre-defined ranks the items to generate a composite ranking of importance. This process is repeated through several iterations until a degree of consensus is reached. Throughout the process the panel members have access to comments and feedback on an anonymous basis. Although final consensus may not be reached, after several iterations, typically one or more groupings of items are discernable.

Kendall's Coefficient of Concordance (Kendall's W) was used to judge the degree of consensus achieved in each iteration (round) of the Delphi process. Kendall's W is a non-parametric statistic that measures the degree of agreement in a ranked list [8]. The statistic may range from 0, indicating no agreement to 1 indicating unanimous agreement. Typically, values over .7 indicate strong agreement [8]; however values between .5 and .7 are considered robust in most circumstances [9]. Participants in the Delphi panel ranked the items presented after each round of deliberation, whereupon the Kendall W statistic was computed. Termination of the process occurs when Kendall's W achieves a strong degree of consensus (greater than .7), a decrease of agreement in subsequent rounds, or indicators of panel exhaustion that would greatly reduce the number of panelists in future rounds [8].

Since the focus of this study is on undergraduate student perceptions, a panel composed of college students enrolled in a junior level business course of a small, rural southern university was created. The panel included 22 undergraduate students, 86.4% of whom were between 18 and 29 years old. Of the 22 students, 13 were male and nine were female. Therefore, the panel was representative of one of the demographic groups that engage in widespread use of social media.

This study used a seeded list approach where students were presented with an initial list of social media risks derived from literature. The list of risks, including definitions, presented to the panelists is included in Appendix A. Panelists were asked to identify the most important or critical social media risks presented to them, and select the top ten risks. In the first round, the panelists did not rank order the risks. The first round focused on winnowing the number of risks to the most frequently identified so that ranking of importance could be completed in subsequent rounds. Risks were presented to the panelists on a random basis. During the process, panelists were given the option of suggesting new risks not present on the seed list.

In the second round, panelists were asked to rank the risks they identified in round one. The list of risks to be ranked included any risk that received 50% of the votes in round one, or that was suggested by the panel in that round. Panelists ranked the risks from most to least critical. In addition to ranking the risks, panelists also had to give their reason for selecting their highest ranked, most critical risk.

In subsequent rounds, panelists reviewed the responses from other panelists for their selection of a most critical risk. Based on this information, panelists were asked to reconsider their risk rankings. In each round, each panelist ranked the risks on the list from most to least critical; adjusting their rankings based on the information presented from other panelists. The panelists' rankings were then analyzed with Kendall's W statistic calculated after each round. In these rounds, the risks were rank ordered based on the previous round. Panelists were also provided the average rank, standard deviation, and Kendall's W statistic.

Upon completion of the Delphi process, the panelists were presented with the results of their deliberations. As these were students enrolled in a class, the Delphi process itself and the results were discussed. For the purposes of the class the discussion revolved around the use of the Delphi technique as a risk assessment approach.

4. Results

Figure 1 presents the Kendall's W statistic over the course of the Delphi ranking rounds. The entire process consisted of four ranking rounds. The degree of consensus increased steadily over the first three ranking rounds achieving peak consensus in the third ranking round. The Kendall's W statistic was calculated at .585 indicating moderately strong agreement. A fourth ranking round was conducted; however, Kendall's W decreased to .562 indicating termination of the Delphi process was warranted. This was confirmed through feedback from the panelists.

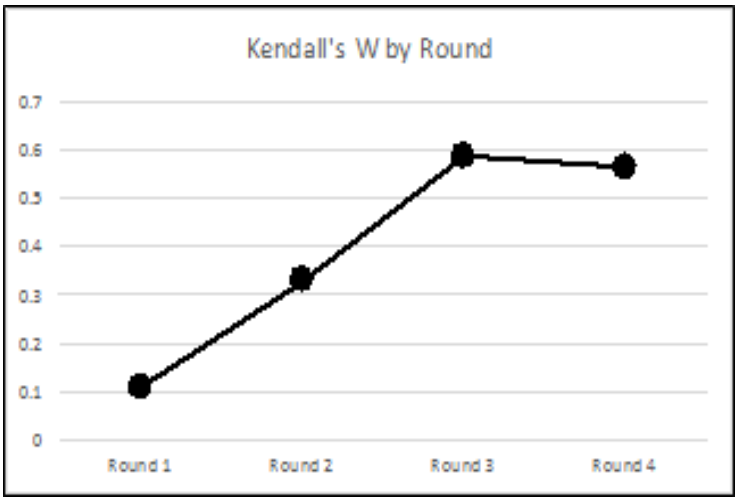

Figure 1. Kendall's W Statistic by Ranking Round

The Delphi panel results for all rounds are presented in Table 2 with the mean rank of each risk item. The panelists were concerned that social media profiles could be used for social engineering and identity theft attacks. One of the panelists suggested the identify theft could lead to other risks (e.g. Damage to reputation and Unintended exposure of information). The reasoning for this was explained as: "*I found identity theft to be the most important 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.*"

Rank	Risk	1	2	3	4
1	Online content may be used for identity theft	4.64	3.14	2.30	2.17
2	Hacks/ unauthorized access to social media accounts	4.32	3.43	3.00	3.11
3	Source of information for hackers/ social engineering	5.23	4.95	3.90	4.28
4	Damage to reputation	5.95	5.29	4.90	4.50
5	Cyber-stalking	5.73	5.19	4.95	5.17
6	Unintended exposure of information	5.36	5.62	5.45	5.61
7	Online content may facilitate discriminatory hiring practices	6.68	6.43	6.35	6.56
8	Cyber-bullying	6.23	6.81	7.80	7.17
9	Malicious software/ malware	6.91	7.95	8.00	8.28
10	Online content shared with unintended third parties for commercial purposes	7.00	8.29	9.30	9.28
11	Online content may be stored or indexed	7.95	8.90	10.05	9.89
	Kendall's W	**.108**	**.328**	**.585**	**.562**

Table 2. Delphi Panel Results - All Ranking Rounds

The second largest risk from social media was the potential for Hacks/ Unauthorized access to social media accounts, where an individual's password is manipulated to obtain access to a personal account. Panelists identified a potential legal risk in that social media content might be used for discriminatory hiring practices. The risk of malicious software/malware was not seen as important by this panel, nor was the sharing of online content with third parties. Finally, panelists did not perceive the storage and indexing of online data to be a critical risk.

5. Discussion

As a group, the panelists identified a diverse set of potential personal social media risks. Perhaps because of the emphasis on personal risk, the panelists in this study differed in their risk rankings from those of the LIS experts mentioned earlier. Although there is some agreement between the two ranked lists (for example identity theft is ranked highest on both lists), agreement breaks down as you move down the lists. Other than some agreement in the rankings for cyber-stalking or cyber-bullying, there is considerable disagreement between the results of these panels.

This study focused on student perceptions of personal risk in using social media. These perceptions are most likely influenced by news media coverage of negative incidents involving the use of social media. Incidents that draw news media attention do not necessarily reflect the range and severity of risks incurred in using social media. As a result, our panelists' rankings are most likely distorted by their exposure to news stories and anecdotes.

The LIS professionals study [7] paints a broader picture of the risks involved in using social media. While the current study may not be definitive, it presents a telling contrast between the panelists' personal views and those of professionals. From an educational perspective, this is an undesirable outcome.

5.1 Implications for Pedagogy

The studies described and cited in this paper identify a need for a systematic pedagogical approach to educate students about the personal risks of using social media. The findings of this study indicate that undergraduate students, who are prospective employees [2], are likely to use social media extensively. The results indicate that pedagogical efforts be directed to address this concern with all students, especially for students specializing in information security.

Educational institutions enroll new students every year. Typically, students engage in various orientation and familiarization activities. This might be a good point at which to introduce students to the risks of using social media. This message should be

reinforced as students advance in their academic career, with emphasis on the identity theft and reputational risks incurred. In particular, the reputational risks should be emphasized as students apply for internships and during their final year when graduation and job seeking activities are at their peak.

Achieving the goal of developing risk awareness throughout a student's academic career will require a thoughtful and measured approach. Typically educational institutions develop or adopt goals and objectives for the curricular offerings and map these on to required or elective course offerings. The results suggest that one of those goals and objectives be the development of general behavioral risk awareness in all students, with the use of social media as one important aspect of this. Incorporating such changes into curricular offerings will require an increase of awareness among all faculty at an institution, and a sustained and persistent effort. We propose that developing social media risk awareness is a long-term goal that will help prepare undergraduate students for successful careers.

For students who are specializing in information security, though, the results suggest that developing pedagogy addressing the risks inherent in using social media is particularly important. A special emphasis should be placed on the social engineering vulnerabilities inherent in the use of social media. At the heart of all information security vulnerabilities is the human element. To the extent that educators can prepare students to understand human motivation and behavior, they can prepare them to identify and assess the risks faced in all aspects of information security. Social media risks are, in a sense, the intersection between the user's behavior and opportunities for others to exploit that user behavior.

With this in mind, the pedagogical designers of information security education programs may want to consider incorporating more extensive coverage of social engineering or human behavioral issues. Beyond simply learning about existing risks in social media, the results suggest that educators should prepare students to assess the potential risks before they are realized. Whether this comes about through specialized course work, or a shift in emphasis on existing course materials; we propose that it is important to give students a better perspective on human behavior. Ultimately, this may mean developing a branch of information security that specializes in social engineering or human behavior.

6. Limitations

The study presented in this paper is of course limited by its design. The data describing perceptions of individual level social media risks was collected from a small sample of students, who may not be entirely representative of the population of social media users. The purpose of this study was to gain insight into student perceptions and is, therefore, not grounded in a theoretical framework. Also, the initial risks identified via literature may be incomplete as new research continuously expands the understanding of social media. While the Delphi technique used in this study accounted for this concern by having panelists contribute risks not identified within the literature, it is possible that relevant risks may have been missed. Additionally, social media is a rapidly developing field of study and the dynamics of it present considerable research challenges.

7. Conclusion

The current study provides a glimpse into students' personal risk perceptions. Although students may perceive the identified risks, these perceptions may not have a factual basis. Future research is needed to examine the actual versus perceived risks that users of social media face. This study points to the need for raising awareness of the personal risks social media users face. From a pedagogical perspective, this means making social media risk awareness a curricula objective; and then developing the materials and instruction to support that objective. For students specializing in information security, the results of this study suggest that academics should emphasize the study of human behavior and social engineering. The results of this study also suggest that more research of social engineering and human behavior in information security is required. Gaining a better understanding of human motivation and behavior can only lead to better awareness of the risks inherent in the use of social media.

8. References

[1] Kaplan, A. M., Haenlein, M (2010). Users of the world unite! The challenges and opportunities of social media. Business Horizons, 53 (1) 59-68.

[2] Social Networking Fact Sheet. Web, Pew Research Center, (2015). http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet

[3] Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A. and Madden, M. Social Media Update 2014. Pew Research Center, (2015). http://www.pewinternet.org/2015/01/09/social-media-update-2014/

[4] Texas teen tweets herself out of pizzeria job. Web, Fox News Network, LLC, Web, (2015). http://www.foxnews.com/us/2015/02/10/texas-teen-tweets-herself-out-pizza-job/

[5] Fox, S. and Rainie, L. The Web at 25 in the U.S., Pew Research Center, (2014). http://www.pewinternet.org/2014/02/25/the-web-at-25-in-the-u-s

[6] Lenhart, A. Teens, Social Media & Technology Overview 2015. Pew Research Center, Pew Research Center, (2015). http://www.pewinternet.org/2015/04/09/teens-social-media-technolgy-2015

[7] Haynes, D. and Robinson, L (2015). Defining user risk in social networking services. *Aslib Journal of Information Management*, 67 (1) 94-115.

[8] Worrell, J. L., Di Gangi, P. M. and 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.

[9] Brancheau, J. C. and Wetherbe, J. C. (1987). Key issues in information systems management. *MIS Quarterly*, 11 (1) 23 - 45.

Appendix A – Personal Social Media Risk Items and Definitions

Item	Definition
Minority Influence or amplification of events	Creation of a distorted sense of market opinion by increasing the visibility of a vocal and visible minority.
Unintended exposure of information	Accidental transmission and disclosure of information to an unintended third party.
Convergence of personal and professional network	Integration of one's personal and professional life through digital connections, relationships, software applications, etc.
Source of information for hackers/ social engineering	The use of information found on a social media platform to gain unauthorized access to personal resources.
Decreased personal productivity	Reduction in efficiency and/or effectiveness due to social media usage for social or non-work purposes.
Unreliable user-generated content	Creation of content (posts, images, etc.) by users which contains misinformation, errors, or other incorrect data.
Damage to reputation	Use of social media in a manner that diminishes how an individual is perceived by others.
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.
Cyber-bullying	Purposeful acts of harm, which can take the form of harassment, offensive behavior, secret sharing, public embarrassment and humiliation.
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.

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.
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.
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.
Online content may be used for identity theft	Use of information found on a social media platform to impersonate someone else for fraudulent purposes.
Social information overload	Experience of being overwhelmed by the volume of social network information that is presented too quickly to comprehend or absorb effectively.
Perception of social media acceptance/adoption	Concern that an individual may not be adept or savvy at using social media.
Inconsistent personal branding	Image of an individual as portrayed via social media may be inconsistent with the image communicated through more traditional means.
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.
Service interruption	Temporary inability to access social media applications or platforms. Use of fake profiles, postings, blogs or other social media content to secretly install malicious software on a person's computer without their consent.
Malicious software (malware)	Unauthorized use of an individual's social media accounts by a third party with the intent to cause harm.
Hacks / unauthorized access to social media account 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.