Inf Syst Front (2018) 20:1097–1116
DOI 10.1007/s10796-016-9714-2

What could possibly go wrong? A multi-panel Delphi study of organizational social media risk

Paul M. Di Gangi[1] · Allen C. Johnston[1] · James L. Worrell[2] · Samuel C. Thompson[1]

Published online: 11 October 2016

Abstract The growth of social media has crossed the boundary from individual to organizational use, bringing with it a set of benefits and risks. To mitigate these risks and ensure the benefits of social media use are realized, organizations have developed a host of new policies, procedures, and hiring practices. However, research to date has yet to provide a comprehensive view on the nature of risk associated with the use of social media by organizations. Using a multi-panel Delphi approach consisting of new entrants to the workforce, certified human resource professionals, and certified Information Technology auditors, this study seeks to understand organizational social media risk. The results of the Delphi panels are compared against a textual analysis of 40 social media policies to provide a comprehensive view of the current state of social media policy development. We conclude with directions for future research that may guide researchers interested in exploring social media risk in organizations.

Keywords Social media · Organizational risk framework · Social media policy · Risk · Web 2.0 · Information security

✉ Paul M. Di Gangi
pdigangi@uab.edu

[1] Department of Management, Information Systems, and Quantitative Methods, Collat School of Business, University of Alabama at Birmingham, 1150 10th Ave S., Birmingham, AL 35294-4460, USA

[2] Department of Accounting and Finance, Collat School of Business, University of Alabama at Birmingham, 1150 10th Ave S., Birmingham, AL 35294-4460, USA

1 Introduction

Social media represents a powerful medium for connecting organizations with their customers (Kane et al. 2009; Kietzmann et al. 2011; Dijkmans et al. 2015; Hanna et al. 2011), understanding customer interests (Baur Forthcoming; Yan et al. 2015), obtaining new ideas about products and services (Di Gangi et al. 2010; Gallaugher and Ransbotham 2010), fostering communication and collaboration among employees (Leidner et al. 2010; Teo et al. 2011; Kane 2015b), and creating business value (Culnan et al. 2010; Lundmark et al. Forthcoming). Social media 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 (p. 61)*" (Kaplan and Haenlein 2010). While the organizational advantages of using social media are clear, a growing concern among scholars and practitioners is how social media introduces new organizational risks (van Zyl 2009; Kane 2015a; Di Gangi et al. 2010; Kane et al. 2009). For instance, an employee tweeting inappropriately from the official Red Cross account about Dogfish Head beer and being intoxicated raised serious public concerns about Red Cross' decision-making and hiring practices.[1]

Incidents such as inappropriate tweeting may appear infrequent, but social media is growing in its adoption and influence within organizations and the opportunities for inappropriate social media use grow as well. Calls for a more social organization (Deans 2011; Kane 2015a; Gaines-Ross 2013; Bharati et al. 2014), from line employees to chief executives, introduces greater opportunities for social media missteps. When a social business strategy is combined with a new generation that has "grown up digital" (Tapscott 2008) and is accustomed to working collaboratively via social media

[1] http://mashable.com/2011/02/16/red-cross-tweet/ (Accessed 05/15/2016)

(Kane 2015a; Leidner et al. 2010; Miller-Merrell 2012; Mooney et al. 2010; Guitierrez et al. 2016), the likelihood increases that organizations in the future will need to maintain a watchful eye over the use of social media. We define *organizational social media risk* as *the potential for negative exposure associated with the use of social media that can have detrimental impacts upon an organization.*

While social media is relatively new to organizations, assessing organizational risk has enjoyed a rich history in both research and practice (Goodhue and Straub 1991; Hogben 2007; Jenkins 2012; Johnston and Warkentin 2010; Johnston et al. 2015; Krasnova et al. 2009; Schmidt et al. 2001; Straub and Welke 1998). Central to this process is the perception of risk associated with a phenomenon (e.g., organizational social media use) and the unique contextual elements (e.g., security controls available in the organization and individual differences relating to the experience of managers with the phenomenon) that may influence how the organization perceives risk (Dhillon and Torkzadeh 2006; Goodhue and Straub 1991; Straub and Welke 1998). The majority of research has focused on the perceptions of risk at the individual level (i.e., risk to the individual using social media) rather than at the organizational level where security policy and adoption decisions are made and applied (e.g., boyd 2008; Jenkins 2012; Miller-Merrell 2012; Aula 2010; Kaplan and Haenlein 2010; Krasnova et al. 2009, 2015; Levy et al. 2015; Saridakis et al. 2016). Few studies have assessed the negative impact of, or risks associated with, the use of social media by organizations (Kaplan and Haenlein 2010; Krasnova et al. 2009; van Zyl 2009; Aula 2010). This is largely because the majority of security research focuses on individual risk perceptions and not the collective perceptions of multiple stakeholders that play a role in defining security strategy and policy at the organizational level. Prior research suggests a variety of stakeholders play a role in the shaping of security policy (Willison and Backhouse 2006); such as, employees, management, human resource (HR) departments, and Information Technology (IT) auditors. At present, no study has provided a purposeful examination of organizational social media risk perceptions from a multi-stakeholder perspective.

Once risks are collectively identified and assessed, organizations can implement security controls that minimize potential disadvantages, (e.g., public exposure of employee misbehavior) while maintaining the spirit of social media in terms of fostering relationships and shared experiences. For instance, one recent approach is to adopt enterprise social media where organizations utilize internal social media platforms, thereby limiting risks to within the organizational boundary (Kane 2015b; Leonardi et al. 2013). While this approach limits risks, it also limits the potential benefits. When adopting external social media platforms that are open to the public, security controls are largely dependent upon the platform providers (e.g., Facebook, Twitter, and LinkedIn). Furthermore, employees may use social media for both professional *and* personal purposes and on non-organizationally owned devices (e.g., personal smartphones), thereby increasing the complexity involved in crafting security policy and engendering compliance. Consequently, social media risk represents a unique phenomenon for scholars and practitioners.

This study evaluates organizational social media risk perceptions from a multi-stakeholder perspective and adapts a framework from existing literature that can be used to guide security research and practice. Specifically, we adapt Straub and Welke's (1998) managerial risk perceptions framework that models the risk perceptions of an organizational manager at the individual level to the organizational level. To accomplish these goals, this study focuses on the following research questions: (1) *What are the risks that social media present to organizations?* (2) *How do organizational social media risk perceptions differ based on organizational employee perspectives?* and (3) *How do organizations currently mitigate social media risks?*

In doing so, this study contributes to literature in several ways. First, this study contributes by extending the risk perceptions literature to the organizational and adapts a well-known model of individual risk perception (i.e., Straub and Welke (1998) managerial risk perceptions model) to study organizational social media risk. This study also contributes to the information security and social media literature streams by focusing on organizational social media risk directly, as opposed to treating specific social media risks as tangential factors in other research studies. This study synthesizes the literature on organizational social media risk and provides a Type 1 theory contribution (i.e., typology of organizational social media risk) for future researchers interested in exploring the negative side of social media. Second, through the vantage of a multiple stakeholder perspective, this study demonstrates the importance of obtaining a holistic view of organizational social media risk based on the variations in risks identified by different stakeholders. By identifying and assessing divergent perceptions of organizational social media risks, we realistically model organizational processes for formulating security policy. This study also evaluates existing risk mitigation techniques related to social media and recommends appropriate policies and procedures for social media use in organizations. Lastly, we provide directions for future research to information security and social media scholars in the areas of social media policy robustness, employee policy compliance, and security education, training, and awareness.

The manuscript will unfold as follows. First, we review the literature on social media risks to identify what could possibly go wrong and conceptually segment organizational social media risk into three key areas: social, technical, and legal risks. Following this review, we outline a multi-method approach based upon an extension of Straub and Welke's (1998) managerial perceptions of security risk framework to answer the research questions using (1) a Delphi technique that assesses multiple stakeholder perspectives on the state of organizational social media risk and (2) a textual analysis of existing social media policies that explores whether these policies account for the range of identified risks. We conclude with an analysis of the results and future directions for research.

2 Organizational risk perceptions – a framework

An organization's security posture relies on the accuracy of its risk perceptions (Kotulic and Clark 2004; Rhee et al. 2012). When an organization fails to understand risk or lacks awareness of risk, it cannot develop effective security policies or other appropriate controls to mitigate the danger to the organization (Alter and Sherer 2004; Baskerville et al. 2014). To understand how risk perceptions are formed, Goodhue and Straub (1991) developed a model of security concern based on a manager's attitudes towards the risks inherent in industry, the actions an organization can take to mitigate risk through its' IT environment, and personal expertise and work experience. Straub and Welke (1998) adapted this model to propose a managerial risk perceptions framework based on three dimensions: the organizational environment (i.e., risk inherent in an industry), IS environment (organizational actions to mitigate risk), and individual differences (awareness of risk based on personal work experience).

Since its introduction, the managerial risk perceptions framework has proven useful to researchers exploring incident response handling decisions (Tan et al. 2003), managing risk in technology start-ups (Ng and Feng 2006), and understanding risk perceptions in cooperatives (Goh and Di Gangi 2016). However, the framework has not gained much attention beyond these initial investigations. In fact, its initial evaluation found limited explanatory power which Goodhue and Straub (1991) attributed to sample selection limitations (i.e., general managers that did not manage security functions within an organization). We believe the limitations of the managerial risk perceptions framework can be attributed to two key factors. First, the organizational environment component fails to include risks beyond those inherent to an industry, thereby limiting the value the framework provides to a general level. Second, the risk perception framework functions at the individual level rather than at the organizational level where a mixture of security professionals (e.g., HR and IT auditors) collectively identify and develop a risk control strategy. Social media provides an excellent example of when a technology requires a risk assessment that considers risk from the internal organizational environment (i.e., employees use of social media), in its customer environment (i.e., employees interacting with customers), and from industry in general (i.e., healthcare and financial industry laws and regulations for information disclosure via social media). Furthermore, social media is not a single technology such as email that an organization installs and configures for clearly identified purposes. Instead, social media is a mixture of technologies that are each designed and hosted by a third-party (e.g., Twitter and Facebook) that an organization subsequently uses for its own interests. Recent research suggests social media is not solely an IT manager's responsibility and is likely to perform best when responsibility is shared among a variety of organizational stakeholders (Deans 2011). As a result, the managerial risk perception framework requires adaptation to more appropriately understand organizational social media risk.

Figure 1 depicts the adapted version of the risk perceptions framework to the organizational level. Our adaptation adheres to the spirit of the original theoretical development, while updating its dimensions to reflect the current information security landscape within organizations. First, we modified the organizational environment dimension, which focused on the inherent industry risk, to a broader organizational risk environment encompassing the full risk landscape for an organization that uses social media. In doing so, we stress the need for an accurate risk assessment that moves beyond those inherent to an industry and includes: risks from insiders (Ifinedo 2011), employee use of social media, industry risks (Kankanhalli et al. 2003) such as legal or regulatory issues that arise from the use of social media, and other non-technical risks (Spears and Barki 2010). Second, we modify the individual differences dimension to more accurately depict the risk assessment and planning process that organizations utilize when adopting a new technology. We address the sample concern expressed by Goodhue and Straub (1991) by adopting Willison and Backhouse's (2006) perspective that organizations need to include a variety of different departments or security perspectives when managing risk (e.g., HR and IT auditors). By including a wider variety of perspectives, we believe this will mitigate the issue raised by prior scholars that security has largely been viewed as solely a technical issue with responsibility falling to IT managers (El-Gayar and Fritz 2010). We argue that an organizational security perspectives dimension allows for multiple stakeholders to be involved in information security from technical and non-technical perspectives. The collective perspective that is generated from their inclusion will result in more accurate organizational risk perceptions. The IS environment dimension is renamed to risk mitigation and control capabilities to reflect the variety of controls the field of information security has at its disposal to mitigate risk including technical (e.g., web filtering), physical (e.g., banning of personal mobile devices), and administrative controls (e.g., social media policy).

The primary purpose of this study is to understand the risk that social media present to organizations. We argue that an adapted version of Straub and Welke's (1998) managerial risk perceptions framework to the organizational level allow us to gain a full picture of the risks to organizational use of social media. The next section provides a further analysis of the

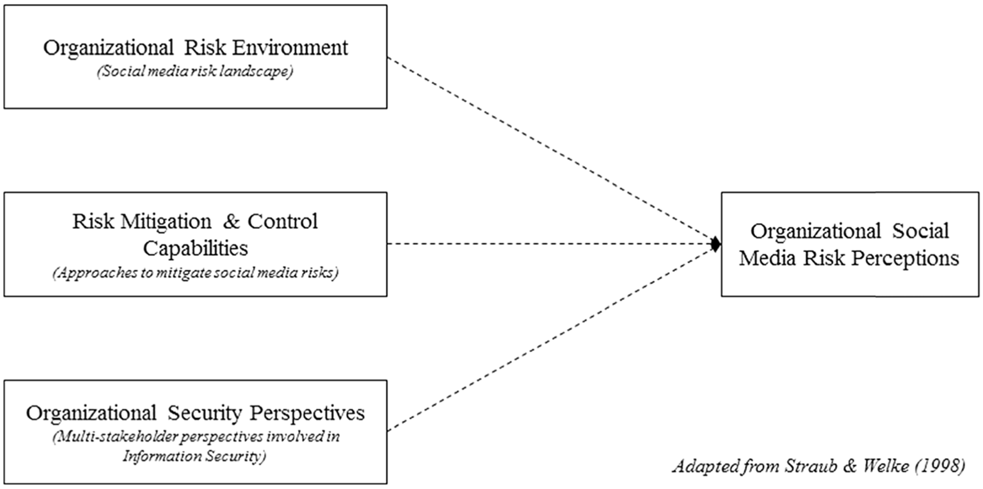
Organizational Risk Environment
(Social media risk landscape)
Risk Mitigation & Control Capabilities
(Approaches to mitigate social media risks)
Organizational Security Perspectives
(Multi-stakeholder perspectives involved in Information Security)
Organizational Social Media Risk Perceptions
Adapted from Straub & Welke (1998)

Fig. 1 Adapted model of organizational social media risk perceptions

literature on the organizational risk environment and develops a typology of organizational social media risk. In the methodology section, we account for the remaining dimensions by including a variety of perspectives from professionals involved in security planning and identify the variety of controls used to mitigate organizational social media risk.

3 Organizational risk environment

While research has primarily explored social media as an intriguing phenomenon with a wide range of potential benefits from knowledge sharing, innovation, communications, and organizational strategy across multiple industries (Dahlander and Piezunka 2014; Kallinikos and Tempini 2014; Kane et al. 2014; Leonardi et al. 2013), social media risks have largely been ignored with the exception of a few notable studies (e.g., Chou et al. 2009; Kaplan and Haenlein 2010; Aula 2010) and, to date, no study has provided a comprehensive synthesis of the literature on social media to identify the potential risks to organizations. Toward mitigating this gap, we followed Templier and Paré's (2015) guidance for conducting a comprehensive literature search to identify all relevant organizational social media risks and then structured those risks within a typology framework. The literature we reviewed were identified as relevant journal articles based on a keyword search using the following search terms: social media, social network, and social networking combined with risk. To maximize the potential pool of results, we did not limit the disciplines. We then filtered our results to identify organizationally relevant studies in order to derive a conceptual framework for understanding an organizational risk environment.

The existing risks identified in this search reflect three dominant risk dimensions within an organizational risk environment – social, technical, and legal. Further, risks present themselves as a result of the organization's interactions with its internal and external environment (Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004; IT Governance Institute (ITGI) 2005), we distinguished between risks originating from internal sources within the organizational boundary (e.g., employee actions) and risks external to the organization (e.g., customer-driven). Similarly, we look at those risks that are native to the internal organizational environment and those that are native to the external organizational environment in terms of the impact of the risk (e.g., an internal risk with an external impact).

3.1 Social risks

Social media is, at its core, a series of technologies that facilitate and enable social interaction among individuals, groups of individuals, and organizations. Social media is perceived as an intimate technology for fostering relationships and growing closer through frequent interaction; and we view the risks associated with these relationships and interactions as social in nature (i.e., social risks). The social risk dimension focuses on organizational risks associated with improper information disclosure, faulty business decisions, social engineering attacks, productivity losses, damage to professional and organizational reputation, cyber-stalking and bullying, or damage to consumer or organizational confidence due to the actions of organizational personnel (Helm and Jones 2010; Kane et al. 2009; Krasnova et al. 2009; van Zyl 2009; Hsu and Lawrence 2015; Byrd 2012). Central to these risks is the organization's employee orientation where the risk is introduced by human action or inaction, whether on behalf of the organization, or as an individual that may be perceived as representing the organization.

Typically, in risk assessment exercises, evaluators first look to threats that originate within the internal organizational environment (Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004; IT Governance Institute (ITGI) 2005). Oftentimes, users of social media discover that their personal and professional online identities "bleed into each other," where what one does on her personal account may affect her professional opportunities (boyd 2008). An example was Cold Stone Creamery's firing of an employee displaying vulgar and racially derogatory remarks about the President of the United States on her personal Facebook account. Even though the posting was not directly connected to Cold Stone Creamery, it caused an uproar in the local community, requiring the organization to take action to align with local norms for employee behavior. As can be seen from the example above, the Internet platform supporting these online interactions can lead to miscommunication of the context surrounding a message (Wesch 2008).

From an organization's perspective, the potential for negative publicity, reputation damage, and loss of revenue poses a significant risk if the organization does not act when employees engage in negative behaviors on their personal social media accounts, behaviors that may be construed as reflecting the views of the organization (Helm and Jones 2010; Kane et al. 2009; Krasnova et al. 2009; van Zyl 2009). Furthermore, because of an employee's online, public opinions and behaviors, an organization may face its own form of cyber-bullying through online petitions and boycotts by its customer base if the employee's views are not aligned with the consensus shared among the organization's customers.

Once internal threats are identified and assessed, evaluators turn their attention to those threats that originate from the external organizational environment. Social media also presents organizations with the opportunity to engage directly with its customers to learn about their needs and interests, thereby serving as a potential business intelligence data source (Di Gangi and Wasko 2009; Kane et al. 2009; Di Gangi et al. 2010; Bernoff and Schadler 2010). However, caution must be exercised as the opinions shared via social media could guide managers towards a poor decision. The Internet affords special interest groups that may traditionally hold a minority opinion an opportunity to approximate a large, popular opinion on an organization's social media sites through coordination efforts (Di Gangi and Wasko 2009; Kane et al. 2009; Di Gangi et al. 2010).

In 2007, Dell launched IdeaStorm to solicit ideas on how to improve its products with several popular ideas involving the adoption of open source software. While potentially valuable in terms of developing a relationship with some of the most ardent supporters of software and hardware, such ideas may not have been oriented towards Dell's primary consumers of traditional laptops and desktops. Consequently, managers can fall prey to a minority position, making business decisions with faulty intelligence that lead to poor product offerings.

Another external social risk associated with social media is the opportunity it creates for criminals and malicious users to gain access to organizational resources or personally identifiable information (PII) through social engineering (van Zyl 2009; Vishwanath 2015). Facebook and LinkedIn users routinely post much of the information needed to verify their identity for personal accounts. Facebook and LinkedIn webpages may display information such as elementary school attended and favorite pets/actors/actresses. Such personal information is useful for an attacker guessing a user's password (Barton and Barton 1984). Furthermore, user posts about events can be used by a malicious user to convince a target of a prior history or shared acquaintance that could legitimize an attacker (i.e., "pretexting"), causing the target to improperly disclose information (Vishwanath 2015). Consequently, social media creates risks to users and organizations based on indiscriminate information sharing.

3.2 Technical risks

The technical risk dimension focuses on the risks inherent in social media platforms and their effects on organizations' IT resources (e.g., end user devices, network resources, etc.). Prior research has highlighted the challenges social media presents to organizations from a technical capacity perspective – defined as the negative impacts upon an organization's technological infrastructure. Individuals that continuously peruse social media sites place excessive strain on an organization's network infrastructure that could impede legitimate business processes (van Zyl 2009). Consequently, many organizations have imposed a ban on such sites through filtering and acceptable use policies. However, both actions require resources to monitor and control behavior, thereby introducing additional strain on IT department resources.

From an external technical risk standpoint, social media platforms are increasingly used as vectors for introducing malicious code (malware) into the organizational computing environment, thereby circumventing traditional security controls to gain unauthorized access to accounts (Hogben 2007). For instance, Twitter may not scan for malicious links in tweets and, due to the 140-character limitation, allows uniform resource locators (URLs) to be shortened using third-party websites. Instead of helpful websites, the shortened URLs provided by malicious users lead to malware that then propagates across personal and corporate systems. Social media platforms are also giving new life to aging internet-based threats. For example, The Federal Bureau of Investigation (FBI) suggests "click-jacking" is the analog to a tactic long employed in email-based attacks: create a legitimate-looking hyperlink and then code the underlying URL to direct the user to a different webpage, download malware, or upload critical user information (usernames, passwords, and the like).[2] The most common click-jacking attacks utilize the "Like" and "Share" functionality in social networking sites to achieve similar malicious purposes.[3]

[2] https://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks (Accessed 05/15/2016)

[3] https://www.zerofox.com/blog/top-9-social-media-threats-2015/ (Accessed 05/15/2016)

3.3 Legal risks

In the context of organizational risk environments, legal risks are defined as risks due to the legal uncertainty of the individual event or legal environment as a whole resulting in loss for an organization (Tsui 2013). As social media technologies have become more stable and accepted as official communication channels, the potential for legal consequences due to inappropriate disclosure of information is heightened. For instance, the Securities and Exchange Commission (SEC) recently modified its disclosure policies to include social media as a method for conveying information to investors and customers.[4] A variety of industries are subject to regulatory acts due to the sensitive nature of their information requirements. These industries and their legislative acts include financial institutions (Gramm-Leach-Bliley Act (Gramm et al. 1999)), healthcare providers (Health Insurance Portability and Accountability Act (Kennedy and Kassebaum 1996)), and educational institutions (Family Educational Rights and Privacy Act (Buckley 1974)), among others. In response to the proliferation of regulatory guidance, affected industries implement extensive control procedures to maintain confidentiality and integrity of relevant information, as well as conformity with applicable legislation and industry guidance.

Improper disclosure of protected information can result in the dismissal of an employee, penalties or fines levied against the organization, and possible revocation of clearances to work on projects. For instance, healthcare organizations have seen the potential advantages that patient support via social media can have on treatment and overall patient healthcare (Sarasohn-Kahn 2008; Johnston et al. 2013). However, organizations operating in the healthcare industry must balance the importance of providing personalized healthcare via social media against regulatory obligations for safeguarding personal healthcare information (e.g., illness, medication, personal history). Failure to adequately protect this information, even from transitory disclosure, can result in significant fines and additional, costly regulatory requirements to prevent future incidents.

Additionally, HR departments across industries are facing new challenges from prospective employees publicly disclosing sensitive information that cannot be used in hiring decisions (e.g., age, gender, ethnicity, and sexual orientation). From an internal risk perspective, social media accounts can be reviewed to assess the overall character of the prospective employee and their qualifications; however, information that may be seen as discriminatory if used in a hiring decision is also readily available. Recently, several states in the United States have introduced legislation banning the ability of organizations to demand access to prospective employees' social media accounts as a hiring requirement (e.g., Louisiana Personal Online Account Privacy Protection Act of 2014).

3.4 Organizational social media risk summary

The risks associated with social media extend beyond simply a channel for customers to vent about poor customer service or products. From a social perspective, questionable social media usage negatively affects how an organization is perceived online. Rather than simply affecting an individual employee's reputation, the consequences of unsavory online behavior may spill over to the employee's organization, where outsiders equate the individual with their employer. Furthermore, social media presents opportunities for misinformation to be fed into an organization's decision making process, resulting in poor decisions and product/service offerings. From a technical perspective, social media creates a new venue for malicious users to gain access to corporate assets, providing a rich repository of information for social engineering attacks. Finally, from a legal perspective, social media provides a ready outlet for the accidental dissemination of information that organizations are legally liable for safeguarding. Each theme presents potential risks to an organization; however, little is known about how an organization perceives the importance of each of these themes.

Based on our analysis of the literature on social media risk, the social dimension has received the greatest attention from scholars and practitioners. However, the use of social media as launch points for malicious software emphasizes the importance that organizations and individuals must place on the technical risks associated with social media. Finally, as people become more open in their communications through social media, these platforms can serve as the means for inadvertently releasing protected and prohibited information, thereby subjecting the organization to sanctions and fines for breaching legal requirements.

4 Methodology

This study employed a multi-method design based on an adaptation of the Straub and Welke (1998) framework to understand organizational social media risk perceptions. To identify the risks social media introduces into the organizational environment, we employed a multi-panel, seeded, ranking-type Delphi study to better identify and prioritize social media risks within the organizational environment. We adopted the multi-panel approach to capture multiple stakeholders that would be involved in the creation of security policy and compliance procedures within an organization. Lastly, the Delphi panelists were also asked a series of open-ended questions to identify all applicable security controls within the IS environment (e.g., technology-based network filtering/ monitoring, security education, training, and awareness, and administrative policy). Based on panelist responses, we utilized textual analysis of 40 publicly available social media policies to compare against the social media risks identified in the Delphi study to

[4] https://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171513574 (Accessed 05/15/2016)

highlight gaps in current social media policy coverage and areas in need of future research. Each component of our multi-method design is discussed in greater detail below.

4.1 Delphi methodology

To identify the key risk factors associated with social media and the importance of these risks, we conducted a seeded, ranking-type Delphi study using three distinct panels: new entrants into the workforce, HR professionals, and IT auditors. Prior research supports the role of user participation in shaping security policy, suggesting the need to obtain multiple stakeholder perspectives and accurately assess organizational social media risk perceptions (Spears and Barki 2010). The new entrants group was composed of students in both undergraduate and MBA programs who represent typical new hire employees and/or middle managers to gain an employee and general manager perspective on the use of social media. The HR group was composed of new and seasoned HR professionals whose interests in social media align with personnel issues, including hiring, employee development, and termination. The IT auditors group was composed of new and seasoned IT auditors whose interests in social media align with assessing the efficiency and effectiveness of technology-related risk management activities within the organization.

The Delphi method was chosen as it is a structured, iterative group decision process where a fixed-sized panel of individuals are tasked with reaching consensus on a specific task or issue (Linestone and Turoff 2002). It has been used extensively within the information systems, accounting, marketing, and management fields to assess the importance of specific issues and provide guidance on how to best approach a problem or task based on collective opinions (Best 1974; Brancheau and Wetherbe 1987; Brockhoff 2002; Dickinson et al. 1984; Schmidt et al. 2001; Worrell et al. 2013; Brancheau and Wetherbe 1990; Gray and Hovav 2014). This method has been demonstrated to be effective in distilling a diverse group of issues into a refined, prioritized list that can be used as a basic framework for additional inquiry (Linestone and Turoff 2002; Schmidt 1997).

4.2 Panel selection and composition

As the quality of results of a Delphi study is predicated on the suitability of the panelists used, the selection process for panelists is crucial. We utilized a multi-panel design, with each panel designed to obtain unique perspectives on organizational social media risk. Taking into account multiple perspectives in identifying and addressing risk is key, as different stakeholder groups often perceive technology-related risks differently (Hunton et al. 2004; Reich and Benbasat 2000). While there is no *ideal* size for a panel, extant literature suggests that panels with sizes between 10 and 30 participants are appropriate, with smaller panels being sufficient under ideal conditions (Brockhoff 2002; Delbecq et al. 1975; Paliwoda 1983; Worrell et al. 2013). Moreover, in multi-panel settings such as this study, there is no requirement that the panels have similar number of participants (Schmidt 1997). Each panel member was asked for their perceptions of risk for organizations using social media.

The new entrants panel was segmented into two sub-panels: undergraduate and MBA students. The undergraduate panel included 22 undergraduate students enrolled in a project management course focused on the operational elements of project management (including an understanding of risk assessment and mitigation from a project perspective). The students were majors in accounting, business administration, entrepreneurship, information systems, international business, and marketing. This panel was derived from a rural, small-sized southern university and was composed of 13 males and 9 females with 86.4 % between the ages of 18 and 29. The MBA panel included 29 graduate students enrolled in a special topics course focused on the strategic impact of social media on business processes and outcomes. The panel originated from an urban, medium-sized southern university and was composed of 12 males and 17 females with 69 % between the ages of 18 and 29. The MBA students were employed in industries including: education, energy, finance, healthcare, non-profit, technology, consulting, and transportation. We deemed segmentation into two sub-panels appropriate so as to tap into the social media risk perspectives of those taking entry-level positions (i.e., undergraduates) as well as those assuming new middle management positions (i.e., MBAs).

The HR professionals panel was segmented into two sub-panels: those with less than five years of experience in the field as a Professional in Human Resources (Under Five Years PHR) and those with over five years of experience (Over Five Years PHR). The PHR is a certification sponsored by the Human Resources Certification Institute (HRCI). Professionals that possess the PHR certification have demonstrated mastery of the technical, operational and regulatory aspects of the HR profession in the United States. The certification requires HR professionals to meet minimum educational and experience requirements, as well as passing a computer-based exam, in addition to adhering to rigid continuing education requirements. Areas covered in the PHR body of knowledge include: (1) business management and strategy, (2) workforce planning and employment, (3) HR development, (4) compensation and benefits, (5) employee and labor relations, and (6) risk management.

The Under Five Years PHR panel was composed of 13 HR professionals. Ten were female and three male, with all panelists possessing at least an undergraduate degree (four with graduate degree) with an average age of 37 years. The average years certified was 2.2 years with 11.4 years of relevant work experience in industries including: technology consulting, government, insurance, manufacturing, architecture, agriculture, and healthcare. The Over Five Year PHR panel was composed of 12 HR professionals, eleven females and one male. All panelists possessed at least an undergraduate degree (three had graduate degrees) with an average age of 46.3 years. The average years certified was 8.7 with 16.2 years of relevant work experience in industries including: technology consulting, government, insurance, manufacturing, healthcare, consumer electronics, and retail.

The IT auditors panel was similarly segmented into two groups: those with less than five years' experience in the field as a Certified Information Systems Auditor (Under Five Year CISA) and those with over five years' experience (Over Five Year CISA). The Certified Information Systems Auditor is sponsored by the Information Systems Audit and Control Association (ISACA) and is the most widely recognized global certification for IT auditors. These certified IT auditors have demonstrated mastery in the governance, risk and control of information systems, as well as a variety of techniques used to provide objective assurance on the efficiency and effectiveness of IT risk management practices. As with the PHR, the CISA requires IT auditors to meet minimum educational and experience requirements, as well as passing a computer-based exam, in addition to adhering to rigid continuing education requirements. Areas covered in the CISA body of knowledge include: (1) process of auditing information systems, (2) governance and management of IT, (3) information systems acquisition, development and implementation, (4) IS operation, management and support, and (5) protection of information assets.

The Under Five Year CISA panel was composed of nine IT auditors. Four were female and five male, with all panelists possessing at least a graduate degree with the exception of one panelist (high school degree). This panel had an average age of 36.1 years. The average years certified was 1.9 years with 10.8 years of relevant work experience in industries including: technology consulting, government, finance, and manufacturing. The Over Five Years CISA panel was composed of 19 IT auditors, five females and 14 males. All panelists possessed at least an undergraduate degree (13 had a graduate or professional degree) with an average age of 43.6 years. The average years certified was 10.4, with 15.3 years of relevant work experience in industries including: technology consulting, consumer electronics, education, energy, finance, government, and healthcare.

These panels were selected because each represents a unique perspective on risks associated with social media usage in an organizational setting. The new entrants panels were selected because they represent the immediate future of the workforce with limited experience of the impact social media has had on organizations and the strategic importance of communication channels to business operations. The HR panels were selected because they represent the group often charged with on-boarding new employees, providing the initial introduction to the climate and culture of the organization, crafting new organizational policy, and addressing personnel issues that arise throughout the employment life cycle. The IT auditor panels were chosen because they are charged with providing an independent, unbiased assessment on organizational policies and practices with respect to IT-related risk identification, assessment, and mitigation. Collectively, these panels should provide a well-rounded view of social media risk in organizations.

4.2.1 Social media risk seed

The seeded Delphi method uses an initial list of risks based on prior literature to provide a starting point for the panelists (Schmidt et al. 2001; Worrell et al. 2013). We looked to both practitioner and academic outlets for guidance on creating our initial seed list. For social media risks identified in the literature, our inclusion criteria was based on whether the manuscript focused on social media, social networks, or social networking and included discussion of risks, dangers, or negative consequences of social media usage by an organization. We also identified risks that could potentially occur when a benefit of social media was identified. Lastly, we incorporated risks identified through the authors' industry expertise and professional experiences. Our initial seed list of factors included 22 organizational risks of using social media (see Appendix).

4.2.2 Data collection and analysis method

Panelists were assigned to their applicable panel and emailed a link to a web-based survey containing a randomized list of the initial 22 organizational risks with definitions. Each panelist was asked to identify the ten most important social media risks for organizations (Brancheau and Wetherbe 1987; Dickinson et al. 1984; Brancheau and Wetherbe 1990). The lists were randomized to reduce the likelihood of selection bias. In addition to this initial reduction, we also requested panelists to identify and define any additional risks that are important to an organization. The panelists identified no additional risks, which suggests the identification approach was exhaustive.

Upon receiving the results of the initial solicitation, a reduced list was created for each panel by carrying forward any risk that the majority (50 % or more) of the panel indicated as important (Schmidt 1997) and dropping the remaining risks. Each panelist received the reduced list, rank ordered based on the percentage selected in the initial round and was asked to rank each item from most important to least important. At the end of this round, the mean rank for each risk was calculated as well as Kendall's Coefficient of Concordance (Kendall's W), to determine the degree of consensus for each panel (Schmidt 1997; Worrell et al. 2013).

Additional rounds were conducted with the panelists presented the re-ranked risks based on the mean rank calculation in the previous round as well as a brief synopsis of the justifications provided by each panelist. Each round displayed the current ranking, mean score, and commentary to afford each panelist the opportunity to adjust their rankings according to the panel's overall perspective. This process repeated until (1) consensus was achieved as indicated by a Kendall's W suggesting strong consensus (W > 0.7), (2) a plateau was reached where subsequent rounds were unlikely to increase consensus, or (3) indications that exhaustion of panel member participation had been reached.

4.3 Qualitative analysis

In addition to the ranking process, panelists were asked a series of open-ended questions during each round of the Delphi to obtain further information about how social media risks should be managed by organizations. The first ranking round of the Delphi asked panelists to explain their rationale for selecting the most important social media risk (as done by prior researchers, such as Boje and Murninghan 1982). These responses were used to provide guidance to the researchers in interpreting the rankings from each panel.

In the third Delphi round, we asked panelists to identify the best mitigation technique for reducing social media risks (e.g., education, training, awareness, and policy documentation). Social media policy was the most frequently referenced mitigation technique. Therefore, we collected a random sample of 40 publicly available social media policies from organizations representing the consulting, consumer goods, finance, government, healthcare, media, non-profit, retail, semiconductor, and computer hardware and software industries. These policies were found using the website http://socialmediagovernance.com which maintains a database of social media policies for a variety of organizations.

Two graduate assistants then conducted a qualitative analysis under the supervision of the lead author to code each social media policy based on the three themes (social, technical, and legal/regulatory). Each assistant was given the definition of the risk and each theme and was then asked to indicate presence or non-presence of the risk. Six initial policies were used to assess inter-rater reliability using the percent agreement technique suggested by Boyatzis (1998). Percent agreement takes the overall number of coded items that were identical between the two coders and divides it by the total number of possible codes. In this case, of the 156 possible codes, 125 codes were identical, leading to a percent agreement value of 80.1 %. This suggests moderately strong inter-coder reliability (Boyatzis 1998). In addition, we calculated a Kappa statistic to determine the difference between how much agreement is actually present compared to how much agreement would be expected to be present by chance alone (Viera and Garrett 2005). The Kappa statistic indicated good agreement with 61.1 % agreement (Landis and Koch 1977). Each assistant subsequently coded the remainder of the social media policies with the lead author conducting a random check to ensure continued reliability. The results of the coding were then used to compare the final rankings of the Delphi panel against the current social media policies to determine gaps and/or consistencies.

The fourth round focused on identifying the incentives and disincentives that organizations can use to encourage compliance with social media risk policies and other controls. The question used in our discussion on mitigation techniques was, "*To enforce social media policies, what are the most appropriate incentives and disincentives to ensure employee compliance?*" An author was responsible for reviewing the responses and summarizing the overarching sentiment of the responses across the panels. The lead author subsequently verified these findings by reviewing all question responses.

5 Results

This next section outlines the results of the Delphi panels, the open-ended question for mitigation techniques, and the analysis of social media policies based on the findings from the Delphi panels.

5.1 Delphi panels

Final results of the social media risk factor rankings for each panel are presented in Table 1. Italicized social media risks represent the risks identified across all panels. Overall, 18 unique risks were identified with 6 risks common across all six panels. Furthermore, all three themes for social media risk were found within the final rankings. However, social risk was the dominant theme in comparison to legal and technical risk.

In terms of the overall risks, six risks were identified across all panels. All common identified risks were social with the exception of one legal risk; the *Purposeful loss of competitive data or trade secrets (Average ranking 4.5)*. It is interesting to note that the remaining social risks demonstrate a diverse understanding of risk in terms of both internal via *Decreased productivity (Average ranking 6.8)* as well as external impact which was recognized as the most common social risk. For instance, *Unintended exposure of information (Average ranking 2.6)* was the most important overall risk with three of the six panels specifically identifying it as the most important risk facing organizations. This is likely because the unintended exposure of information may be seen as a general risk that incorporates many of the other risks associated with social media use. For instance, exposing a customer's personal information unintentionally will likely result in *Damage to organization's reputation (Average ranking 2.8)* as well as

Table 1 Delphi panel results

Risk Rank	Panel					
	Undergraduate	MBA	Under five year PHR	Over five year PHR	Under five year CISA	Over five year CISA
1	Purposeful loss of competitive data or trade secrets (LI)	Damage to Organization's Reputation (SI)	Damage to Organization's Reputation (SI)	Damage to Organization's Reputation (SI)	Unintended Exposure of Information (SI)	Intentional or Unintentional Violation of Legal or Regulatory Requirements (LI)
2	Damage to consumer confidence (SI)	Purposeful loss of competitive data or trade secrets (LI)	Unintended Exposure of Information (SI)	Decreased productivity (SI)	Purposeful Loss of Competitive Data or Trade Secrets (LI)	Unintended Exposure of Information (SI)
3	Damage to Organization's Reputation (SI)	Unintended exposure of information (SI)	Intentional or Unintentional Violation of Legal or Regulatory Requirements (LI)	Unintended Exposure of Information (SI)	Source of Information for Hackers/Social Engineering (SE)	Damage to Organization's Reputation (SI)
4	Decreased productivity (SI)	Inconsistent branding (SI)	Employee Views Perceived as Sanctioned/Approved by Employer (SI)	Employee Views Perceived as Sanctioned/Approved by Employer (SI)	Hacks/Unauthorized Access to Social Media Account (TE)	Damage to consumer confidence (SI)
5	Unintended exposure of information (SI)	Damage to consumer confidence (SI)	Damage to consumer confidence (SI)	Inconsistent Branding (SI)	Intentional or Unintentional Violation of Legal or Regulatory Requirements (LI)	Source of Information for Hackers/Social Engineering (SE)
6	Source of information for hackers/social engineering (TE)	Decreased productivity (SI)	Inconsistent branding (SI)	Damage to consumer confidence (SI)	Malicious Software/Malware (TE)	Employee Views Perceived as Sanctioned/Approved by Employer (SI)
7	Hacks/unauthorized access to social media account (TE)	Intentional or unintentional violation of legal or regulatory requirements (LI)	Online Content May Facilitate Discriminatory Hiring Practices (LI)	Purposeful Loss of Competitive Data or Trade Secrets (LI)	Employee Views Perceived as Sanctioned/Approved by Employer (SI)	Purposeful Loss of Competitive Data or Trade Secrets (LI)
8	Employee views perceived as sanctioned/approved by Employer (SI)	Hacks/unauthorized access to social media account (TE)	Purposeful Loss of Competitive Data or Trade Secrets (LI)	Malicious Software/Malware (TE)	Damage to Organization's Reputation (SI)	Malicious Software/Malware (TE)
9	Online content may facilitate discriminatory hiring practices (LI)	Employee views perceived as sanctioned/approved by Employer (SI)	Malicious Software/Malware (TE)	Uncontrollable Actions (SE)	Decreased Productivity (SI)	Decreased Productivity (SI)
10	Malicious software/malware (TE)	Unreliable user-generated content (SE)	Damage to Employee Morale (SI)	Inefficient Use of Employer Network Resources (TI)	Damage to consumer confidence (SI)	Inconsistent Branding (SI)
11		Inefficient use of employer network resources (TI)	Decreased Productivity (SI)	Intentional or Unintentional Violation of Legal or Regulatory Requirements (LI)	Inconsistent Branding (SI)	Hacks/Unauthorized Access to Social Media Account (TE)
12				Source of Information for Hackers/Social Engineering (SE)	Inefficient Use of Employer Network Resources (TI)	
13				Online Content Shared with Unintended 3rd Party for Commercial Purposes (SE)	Unreliable user-generated content (SE)	
Consensus	0.651	0.694	0.745	0.829	0.633	0.580
Sample	18	25	13	12	9	19

Italicized risks represent risk identified across all panels

Risk Type: *S* Social, *T* Technical, *L* Legal, Risk Source Orientation: *I* Internal, *E* External

Damage to consumer confidence (Average ranking 5.3) as customers lose trust in an organization's protection of their information. All of these risks, while driven by employee actions, are externally oriented in terms of their potential impact (e.g., consumer perceptions about organization).

It was also interesting to see the inclusion of *Employee views perceived as sanctioned/ approved by employer (Average ranking 6.3),* as this represents a rather complex risk for organizations. While it is externally-oriented in terms of how the risk affects the organization (e.g., Cold Stone Creamery employee example described earlier), the risk itself may be external to the organization as well since an employee's views on personal social media accounts are beyond the control of the organization. Thus, this risk represents an internal threat from its employees as well as an external threat that has the potential to harm the organization in an uncontrollable manner unless the organization can mitigate personal employee behavior. For instance, one Over Five Year CISA panelist stated "*employees do not often distinguish between when they are acting on their own behalf versus the company's behalf.*" An undergraduate panelist expanded on this notion, "*When people post stuff online it still has an impact on the employer because that person is part of that company. So even at home during personal time anything that you post is going to reflect off of your company as well.*"

When comparing the six panels, two additional observations emerge. First, only the Undergraduate and Under Five Year PHR panel identified the potential for online content to be used to facilitate discriminatory hiring practices (9th in Undergraduate and 7th in Under Five Year PHR panel). As undergraduates represented the youngest panel and most commonly associated with the use of social media, it appears "growing up digital" does not have only positive benefits, but also negative consequences that are being felt by panelists as they enter the workforce and apply for positions. The Under Five Year PHR panel may also be sensitive to this issue as their average age places them on the cusp of the millennial generation and makes its members likely candidates for handling the social media issues of prospective employees. As one HR professional noted, discriminatory hiring practices using social media seems "*the most common and difficult to defend*" risk for HR departments.

Second, when the Undergraduate panel is removed from the set of panels, two additional risks emerge as common among the remaining panels. These panels can arguably be identified as the business professional panels with undergraduates who are business students in the learning phase of becoming a professional. The two additional risks suggest the business professional panels have a greater degree of sensitivity to the financial implications of negative social media use and strategic linkages between the various social risks. Several panelists cited concerns of the costs of social media due to liability considerations "*or discourages a customer from buying from the company*" (Under Five Year PHR), when embarrassing organizational disclosures become public. All of the business professional panels identified the risk of *Intentional or unintentional violation of legal or regulatory requirements* (7th in Graduate, 3rd in Under Five Year PHR, 11th in Over Five Year PHR, 5th in Under Five Year CISA, and 1st in Over Five Year CISA). Legal or regulatory violations typically carry hefty fines in addition to the impact on the organization's reputation, consumer confidence, and branding efforts. All of these assets, if harmed due to social media, can lead to significant financial loss.

Moreover, the business professional panel also included the risk of *Inconsistent branding* (4th in Graduate, 6th in Under Five Year PHR, 5th in Over Five Year PHR, 11th in Under Five Year CISA, and 10th in Over Five Year CISA) as an important strategic risk. For instance, one Over Five Year CISA panelist commented, "*There is excessive overlap in social media forums, both within and externally. Employees may not always behave, use, consider these forums effects on their organization's clients/ customers thoughts about their company. Employers cannot control, monitor, curtail all possible activity – employees won't always be presenting their best side.*" Such an issue has the potential to be exponentially complex if a strategic approach to branding is not taken. As two Under Five Year CISA panelists suggested "*The #1 issue is inconsistent branding because if a company lets more than one employee post on the social media page, the messages they are sending out may be different.*" and "*a mixed message from employees and the organization it* [sic] *can erode customer confidence.*"

5.2 Risk mitigation and control strategies

A total of 66 responses were received to the question "*What are the best approaches to mitigating social media risks for organizations?*" Of these responses, 40 supported a clear social media policy that is communicated frequently as the best mitigation strategy. As one member from the Over Five Year CISA panel stated, there is value in "*a company policy that is clear and concise and communicated on a regular basis using multiple channels.*" This is aligned with the HR professional panels as well where one Over Five Year PHR panel member stated that organizations should "*have a social media policy that outlines what is acceptable and what is not. Periodic monitoring of company social media sites should become the norm for both management and the IT department. The* *policy should also contain consequences of what happens when an employee is found violating the policy.*" Such statements suggest a concise social media policy that clearly states best practices and should include explicit consequences for failures to comply. In addition, panelists recognize the growth of social media technologies and that generations approach their use differently. The growth of social media and differences in their use are viewed as key drivers for social media policy development. As another member from the Over Five Year PHR panel stated, "*technology changes very quickly – have someone at the forefront to address issues before/as they occur. Take into consideration the use of social media by different generations in the workforce today.*"

While policy was the overwhelming recommendation for mitigating social media risks (40 occurrences), additional approaches were also identified, including awareness (10 occurrences), technical solutions such as monitoring or site blockage (nine occurrences), and education (eight occurrences). In fact, many of the responses recognized the complex nature of risk mitigation when dealing with social media and suggested a multi-faceted approach, such as "*train employees and have a good social media policy. That way employees understand how they should use social media.*" Awareness is critical "*to ensure employees understand that what is said even in a personal context via the Internet may have permanent and long-term consequences.*"

The question, "*To enforce social media policies, what are the most appropriate incentives and disincentives to ensure employee compliance?*" received a total of 66 responses. However, respondents struggled to provide actual incentives for an employee to adhere to policy. Most stated "incentives" are not actually benefits to the employee; rather, they are procedures for reminding and informing employees. For instance, one Under Five Year CISA panelist stated one form of incentives is, "*monitoring social media activities.*" An Over Five Year CISA panelist suggested "*periodic performance reviews*" could be effective incentives for social media policy compliance. Both statements indicate a perspective among CISAs that is policy-focused, rather than employee-focused.

In terms of describing disincentives for social media policy compliance, the Over Five Year CISA panelists were seemingly more nuanced in their suggestions than the Under Five Year CISA panelists. For instance, one Under Five Year CISA panelist suggested "*disciplinary measures*" as effective disincentives, without details as to what the measures would be. On the other hand, an Over Five Year CISA panelist provided a much more descriptive disincentive in suggesting that "*organizations may need also to take a strong disciplinary stance in case of breaches so word of mouth and precedents can be effective deterrents.*"

Both CISA panels demonstrated evidence of a broader perspective on the role of incentives and disincentives and their impact on the organization. For instance, one Over Five Year CISA panelist stated, "*Disincentives will halt outside transparency and potentially reduce morale. Incentivizing via recognition of the strong example of others in the organization with a floor for unacceptable practices may create positive behaviors.*" The PHR panelists are similar in their perspective, yet are seemingly more focused on the difficulties associated with implementing incentives and disincentives. For instance, one Under Five Year PHR panelist stated, "*While it is popular practice to limit social media access at work, smartphones now make this impossible. Instead, companies should clearly articulate and then train employees on the social media policy and legalities, social media etiquette, and perhaps develop/test those by creating internal social media prior to opening their intranets to external social media.*" An Over Five Year PHR panelist echoed this sentiment of policy implementation in stating, "*I believe monitoring of employee's internet use is the biggest disincentive a company can employee [sic] to prevent problems. The company should employee [sic] use of filters as appropriate as well. Only with monitoring and follow up contact with employees who break policy, will all employees hear the message that is, the organization is serious and will enforce the internet policy?*"

5.3 Social media policy textual analysis

The results of the open-ended questionnaire analysis for mitigation techniques indicate social media policy would be the primary technique used by organizations. Consequently, we conducted the textual analysis of 40 organizations' social media policies to determine whether the risks identified and prioritized by the Delphi panels were expressed in existing social media policies. In total, the textual analysis included the policies of consulting firms (3), consumer goods organizations (3), financial enterprises (2), governmental entities (6), healthcare organizations (4), media organizations (6), non-profit entities (3), retailers (4), computer hardware manufacturers (5), semiconductor manufacturers (2), and computer software development firms (2). Table 2 presents the textual analysis results based on all risks identified from the initial seed list by industry, sorted by frequency. Italicized social media risks represent the six risks identified across all six Delphi panels.

In total, the average number of risks identified across all social media policies was 6.93 with computer software development firms having the lowest number of identified risks (5.5/policy) and consulting organizations having the highest

Table 2 Textual analysis results (by Industry)

Item	Risk Type	Consulting	Consumer Goods	Finance	Government	Healthcare	Media	Non-profits	Retail	Computer Hardware	Semiconductor	Computer software	Total	% of Policies
Intentional or unintentional violation of legal or regulatory requirements	LI	3	2	2	4	3	4	3	3	5	1	1	31	77.5 %
Damage to organization's reputation	*SI*	*3*	*2*	*2*	*4*	*2*	*5*	*2*	*2*	*2*	*1*	*1*	*26*	*65.0 %*
Purposeful loss of competitive data or trade secrets	*LI*	*1*	*1*	*1*	*2*	*3*	*2*	*3*	*3*	*5*	*2*	*2*	*25*	*62.5 %*
Employee views perceived as sanctioned/ approved by Employer	*SI*	*3*	*3*	*2*	*2*	*3*	*3*	*2*	*2*	*3*	*1*	*1*	*25*	*62.5 %*
Unreliable user-generated content	TE	2	2	1	2	3	4	2	1	4	2	0	23	57.5 %
Online content may be stored or indexed	SE	2	3	1	3	2	4	1	2	2	1	0	21	52.5 %
Damage to consumer confidence	*SI*	*3*	*1*	*1*	*2*	*2*	*2*	*0*	*2*	*2*	*1*	*1*	*17*	*42.5 %*
Unintended exposure of information	*SI*	*3*	*3*	*0*	*2*	*0*	*1*	*0*	*2*	*3*	*0*	*0*	*14*	*35.0 %*
Online content shared with unintended third parties for commercial purposes	SE	1	1	1	2	2	2	0	2	3	0	0	14	35.0 %
Inconsistent branding	SE	2	0	0	0	1	2	2	3	3	0	1	14	35.0 %
Decreased productivity	*TI*	*2*	*2*	*0*	*2*	*1*	*1*	*2*	*1*	*0*	*0*	*1*	*12*	*30.0 %*
Online content shared with unintended third parties for non-commercial purposes	SE	0	0	2	2	2	1	1	1	2	1	0	12	30.0 %
Uncontrollable actions	TE	0	1	1	2	0	0	2	1	1	0	1	9	22.5 %
Inefficient use of employer network resources	SE	0	0	0	1	1	2	1	0	1	0	1	7	17.5 %
Source of information for hackers/social engineering	SE	0	0	0	2	1	2	0	1	0	0	0	6	15.0 %
Malicious software (malware)	TE	0	1	1	0	0	1	0	2	0	0	1	6	15.0 %
Social mobilization/online activism	LI	0	0	0	1	0	2	1	0	1	0	0	5	12.5 %
Perception of social media acceptance/ adoption	SE	0	0	0	0	0	0	2	1	0	1	0	4	10.0 %
Hacks / unauthorized access to social media account	TE	0	0	0	1	0	0	0	1	0	1	0	3	7.5 %
Online content may facilitate discriminatory hiring practices	LI	0	0	0	0	0	0	0	1	0	0	0	1	2.5 %
Minority Influence or amplifications of events	SE	0	0	0	0	0	1	0	0	0	0	0	1	2.5 %
Damage to morale	SI	0	0	0	1	0	0	0	0	0	0	0	1	2.5 %
Service interruption	TI	0	0	0	0	0	0	0	0	0	0	0	0	0.0 %
# of Organizations		3	3	2	6	4	6	3	4	5	2	2	40	

Italicized risks represent risk identified across all panels

Risk Type: *S* Social, *T* Technical, *L* Legal; Source Orientation: *I* Internal; *E* External number of identified risks (8.83/policy). *Intentional or unintentional violation of a legal or regulatory requirement* was the predominant risk identified across all panels with 77.5 % of all policies cautioning employees about the disclosure of content that may create liability or cause regulatory investigation. Only five other risks were commonly identified in more than 50 % of the social media policies with three identified across all Delphi panel members as important (e.g., *Damage to organizational reputation* 65 %, *Purposeful loss of competitive data or trade secrets* 62.5 %, and *Employee views perceived as sanctioned/ approved by employer* 62.5 %). One risk that was removed from the Delphi panel after the initial round due to a lack of perceptual importance was *Online content may be stored or indexed*. While it was removed after the initial round, it was identified in 23 social media policies. The only other risk identified in over 50 % of all social media policies was *Unreliable user-generated content (57.5 %)* which was identified by both the MBA and Under Five Year PHR panels.

While legal and social risks were fairly well represented in all social media policies, technical risks did not appear to be referenced as often, with only seven policies recognizing the impact social media has on employer network resources and six policies discussing how malicious software/ malware can enter an organization through the use of social media. Taken collectively, it appears that organizational social media policies currently focus predominantly on the legal consequences of social risks that may occur when dealing with customers or the public. Similar to the collective Delphi panel results, technical risks received little to no discussion in the analyzed social media policies. Furthermore, the results of the textual analysis also align with a one-dimensional view of social media as a social risk issue with the majority of policies identifying internal social risks that have potential for external impact. Less than 30 % of the social media policies discussed how the use of social media creates opportunities for negative results on internal organizational operations (e.g., decreased productivity, inefficient use of network resources, source of information for hackers / social engineering, and damage to morale). Such findings suggest that current policies fail to cover the full spectrum of risk associated with the use of social media by organizations.

6 Implications for research and practice

Based on the results of the Delphi panels, the analysis of the open-ended questionnaire, and the textual analysis of current social media polices, this study provides contributions to both research and practice.

6.1 Implications for research

6.1.1 Extension of the managerial risk perceptions framework

A few of the more notable contributions to research provided by this study center on the adaptation and extension of Straub and Welke's (1998) managerial risk perceptions framework. First, we adapt the framework to guide researchers interested in exploring risk perceptions at the organizational level. By taking a multiple stakeholder perspective driven by a consensus building technique (i.e., Delphi), this study realistically models the organizational risk environment where risk assessments and policy development are crafted at the organizational rather than individual level. However, it is worth noting that the variation in the panel results beyond the six commonalities suggests individual characteristics do play a large role in how social media is perceived by an organization. Given PHRs and CISAs affiliate with professional organizations, future research should explore how these organizations shape individual perceptions that drive consensus within their respective professional organizations and subsequently interact with different stakeholders to ultimately shape an organization's policy decisions.

Second, the results of this study provide greater specificity and depth to the organizational risk environment component of the adapted risk perceptions framework. Specifically, Straub and Welke (1998) identify the external organizational environment as a dimension of the complete perspective of risk held by managers. However, our findings allude to an internal dimension, in terms of impact, that encompasses risks within the organization, for instance, productivity loss to employees from their use of social media. This distinction in the organizational risk environment adds depth to our extended Straub and Welke's framework, allowing it to better reflect the risks presented by modern social technologies. In migrating that perspective to an organizational level, we find that the legal risks associated with an organization's industry shape how organizational stakeholders perceive social media risk. We also extend the organizational risk environment to include the customer space that shapes the organization's reputation and brand within an industry, an extension that is based on the external orientation that was the most common form of social media risk identified across all Delphi panels.

Our findings regarding the social risk dimension also suggest that social media may create internal and external issues for an organization in terms of employee productivity and morale and the potential to mismanage customer interactions. This suggests the importance of the internal social environment in shaping the risk perceptions of a manager. In combination, the IT infrastructure and internal social environment represent the bulk of an organization's internal environment. Future research should examine these extensions of Straub and Welke's (1998) model to determine whether social media is a phenomenon-specific instance of this model or whether these constructs provide greater explanatory power in other risk phenomena.

6.1.2 Organizational risk environment typology

Another important contribution of this study stems from its synthesis of existing social media literature and the subsequent provisioning of a comprehensive set of risks associated with organizational social media use. According to Gregor's (2006) theory typology, this sort of contribution constitutes a Type 1 theory contribution (taxonomy/ framework) which seeks to classify and describe commonalities found within discrete observations of a phenomenon. Specifically, we find that the social risk dimension of the organizational risk environment can be further decomposed into two sub-dimensions based on risk orientation (internal and external). While an important initial step, future research must determine the relevant range of this taxonomy and its potential to provide further understanding of social media risk and policy formation. As Weber (2012) notes in his theory assessment framework, the level of a theory may provide insight into its appropriateness for use in exploring a focal phenomenon. For instance, can the taxonomy be applied to individual social media technologies (individual level of analysis) or is it best applied at the group level, which synthesizes the holistic nature of risk associated with social media use to produce a social media policy? Researchers may also consider the use of this taxonomy across multiple levels with individual risk profiles of each social media technology taken into consideration to identify the widest range of vulnerabilities or threats. Thus, further research is needed to determine the appropriate level of analysis for the taxonomy defined here.

6.1.3 Social media policy robustness

While social media is a unique phenomenon, prior research exploring the form or structure of security policies focuses on a more context-free approach. For instance, Goel and Chengalur-Smith (2010) provides a simple metric for assessing security policies based on three dimensions: breadth, clarity, and brevity. The results of this study identified six common social media risks that can be used by researchers seeking to explore the breadth dimension of social media policies. Based on the textual analysis results, three of the six common risks were present in less than 50 % of the sampled social media policies suggesting a lack of (breadth) robustness in current policies. However, the explicit identification of risks should be weighed against the brevity and clarity dimensions of a social media policy. Future research should also investigate the effectiveness of social media policies that explicitly address social media risks versus those that are more wide-ranging. Given social media's unique position for personal and professional purposes, research may suggest social media policies should be crafted differently than more traditional security policies (e.g., acceptable use).

6.1.4 Policy compliance motivation

As noted by the PHR panelists, incentivizing compliance with social media policy is a tricky proposition. Toward this goal, however, several recent studies have examined the role of persuasive communications and deterrence strategies in helping form positive policy compliance behaviors (Johnston and Warkentin 2010; Johnston et al. 2015; Li et al. 2014). These studies have leveraged a variety of theories to underpin their work, notably Protection Motivation Theory (PMT), Fear Appeal Theory, Elaboration Likelihood Model (ELM), and Deterrence Theory. Each of these are individual level theories aimed at understanding how individuals are motivated by persuasive communications (PMT, Fear Appeal Theory, and ELM) or deterrence factors such as formal or informal workplace sanctions (Deterrence Theory). Future research should continue to explore factors that influence individual-level policy compliance, as evidenced by recent calls for papers by the *Journal of Information Systems* (2014) and the *Journal of Information Technology* (2014). However, because social media policies are implemented to mitigate risk associated with a social phenomenon, future research endeavors should also examine group-level policy compliance, the interactive, synergistic capability of a group of individuals to comply with social media policy.

6.2 Implications for practice

The results of this study provide several implications for practitioners. First, the contrasting results of the Undergraduate panel and the MBA and other professional panels provide an opportunity to gain insight into the perspective new employees are bringing into the organization concerning the risks of using social media. HR professionals can use the results of this study to redesign new employee orientation and training workshops to ensure new employees understand how social media use affects an organization. Specifically, HR professionals should stress the legal/ regulatory penalties organizations face when violating a law or regulation that protects intellectual property or personally protected information (e.g., FERPA and HIPAA).

Second, the combined results of the Delphi panels and textual analysis suggest current social media policies are focused on the risk of using social media by an organization where impact is external and with specific focus on the legal/regulatory and social risks. Social media policies should also address the consequences social media use can have on internal organizational operations. Such modifications will lead to more robust social media policies and ensure risks are mitigated for an organization both in terms of its overall operating environment and internal resources.

Lastly, the results of the Delphi panels also highlight the expansion of social media as an attack vector for technical exploitation. While social in nature, several panels identified technical risks suggesting a new attack vector for criminals. Inclusion of technical risks within social media policies as well as training and awareness could help organizations mitigate these risks.

7 Limitations

Delphi studies are meant to provide strategic guidance to focus attention on an ambiguous area of research. While useful, further research is needed to expand on these findings to derive a conceptual framework that can be tested and verified. We believe the results of this study validate an initial conceptual framework focused on the social, technical, and legal risks of social media. However, such a framework must be further tested to determine whether such risks are considered by policy makers when formulating social media policies or choosing to adopt new workplace technologies.

Another limitation of this study is that organizational social media risks were identified through an examination of existing literature and used within their specific context. While valid, such approaches potentially lead to some risks being omitted. For instance, a contextual line can be drawn between social activism that results in a beneficial outcome (e.g., Choudhary et al. 2012) and cyber-bullying (commonly associated with teenagers). Within the organizational context, hactivists can engage in bullying tactics to influence organizational action. In reviewing the identified risks, it is possible such actions would have fallen under a different risk factor (e.g., social mobilization/ online activism) and therefore taken into consideration by the panel members. However, without explicitly identifying hacktivism as a risk, the panelists may have inadvertently discarded its importance.

8 Conclusion

Social media is a technological phenomenon that presents great rewards and risks. By drawing consumers closer and creating more interaction points between employees and an organization's environment, an organization can develop strong ties that may lead to long-lasting competitive advantage. However, failure to consider the risks presented by this emerging medium may lead to a variety of negative consequences. The purpose of this research was to develop a conceptual framework for understanding social media risk, gain insight into the varying ways employees might view organizational social media risks, and a deeper understanding of the current techniques for mitigating these risks. Specifically, this paper sought to determine the risks social media present to organizations and how organizations perceive these risks and ultimately mitigate them. Following a multi-panel Delphi research approach consisting of new entrants to the workforce, certified human resource professionals, and certified Information Technology auditors, the findings of this study suggest that a majority of social media policies do not account for three of the risks that all six panels of our study identified as critically important (i.e., unintended exposure of information, damage to consumer confidence, and decreased productivity). Furthermore, the results of our study show that organizations focus almost exclusively on the legal and social risks associated with social media in their policy efforts and fail to incorporate the many technical risks that our panelists identified as dangerous to organizations. These findings contribute to the risk perceptions literature by elevating the focus from specific tangential social media risk factors to organizational social media risks, demonstrating the value of using multiple stakeholder perspectives to obtain a holistic view of organizational social media risk, presenting existing risk mitigation techniques related to social media and recommendation for appropriate policies and procedures for social media use in organizations, and providing directions for future research to information security and social media scholars in the areas of social media policy robustness, employee policy compliance, and security education, training, and awareness.

Appendix

Table 3 Seed list of social media risk

Item	Risk Domain (Source of Risk)	Definition	Literature Source
Intentional or unintentional violation of legal or regulatory requirements	Legal / Regulatory (Internal)	Inappropriate sharing of personal or professional information that is deemed confidential or privileged by government laws or other regulatory bodies.	(Kane et al. 2009; Levy et al. 2015)
Online content may facilitate discriminatory hiring practices	Legal / Regulatory (Internal)	Use of social media content that is typically deemed inappropriate, unethical, or illegal for the purposes of making hiring decisions or resource assignments.	Author generated – Expansion of legal/ regulatory requirements
Purposeful loss of competitive data or trade secrets	Legal / Regulatory (Internal)	Inappropriate sharing of professional information that is deemed confidential or privileged by a company or organization.	(boyd 2008; van Zyl 2009)
Minority Influence or amplification of events	Social (External)	Creation of a distorted sense of market opinion by increasing the visibility of a vocal and visible minority.	(Helm and Jones 2010)
Unintended exposure of information	Social (Internal)	Accidental transmission and disclosure of information to an unintended third party.	(boyd 2008; van Zyl 2009; Levy et al. 2015)
Social mobilization/ online activism	Social (External)	Ability of a distributed group of individuals or groups to coordinate expressing their opinions and/or interests.	(Kane et al. 2009; Choudhary et al. 2012)
Source of information for hackers/ social engineering	Social (External)	The use of information found on a social media platform to gain unauthorized access to personal or organizational resources.	(van Zyl 2009; Saridakis et al. 2016)
Decreased productivity	Social (Internal)	Reduction in worker efficiency and/or effectiveness due to social media usage for social or non-work purposes.	(van Zyl 2009)
Unreliable user-generated content	Social (External)	Creation of content (posts, images, etc.) by users which contains misinformation, errors, or other incorrect data.	(Kane et al. 2009; van Zyl 2009; Di Gangi et al. 2010; Levy et al. 2015)
Damage to reputation	Social (Internal)	Use of social media in a manner that diminishes how an organization is perceived by others.	(Argenti and Druckenbiller 2004; boyd 2008; Krasnova et al. 2009; van Zyl 2009; Aula 2010; Levy et al. 2015; Hsu and Lawrence 2015; Byrd 2012; Dijkmans et al. 2015; Wakunuma and Stahl 2014)
Employee views perceived as sanctioned/ approved by employer	Social (Internal)	Misperception by individuals, customers and others that a posting by an individual represents the views of their employer.	(Kane et al. 2009; Levy et al. 2015)
Online content may be stored or indexed	Social (External)	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; Levy et al. 2015)
Online content shared with unintended third parties for commercial purposes	Social (External)	Use or transmission of an organization'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	Social (External)	Use or transmission of organization's content to a third party for reasons other than economic gain.	(Krasnova et al. 2009)
Perception of social media acceptance/adoption	Social (External)	Concern that an organization may not be adept or savvy at using social media.	(Mooney et al. 2010; Bharati et al. 2014)
Inconsistent branding	Social (Internal)	Image of an organization as portrayed via social media may be inconsistent with the image communicated through more traditional means.	(Kane et al. 2009; Levy et al. 2015)
Damage to consumer confidence	Social (Internal)	Information disseminated through social media may damage current and potential customers' impressions of a company, its products and/or services.	(Argenti and Druckenbiller 2004; van Zyl 2009; Byrd 2012)
Damage to morale	Social (Internal)	Information disseminated through social media may damage the sense of well-being and faith that employees share regarding their employer.	Author generated – Extrapolation from damage to consumer confidence
Uncontrollable actions	Social (External)	Social media content that is shared or contributed about an organization in a manner that is not under the organization's direct control.	(van Zyl 2009)

Table 3 (continued)

Item	Risk Domain (Source of Risk)	Definition	Literature Source
Hacks / unauthorized access to social media account	Technical (External)	Unauthorized use of an organization's social media accounts by a third party with the intent to cause harm.	(Hogben 2007)
Inefficient use of employer network resources	Technical (Internal)	Negative effects on corporate servers, network bandwidth and other corporate IT resources of employees accessing social media sites.	(van Zyl 2009)
Service interruption	Technical (Internal)	Temporary inability to access social media applications or platforms.	Author generated – IT infrastructure risk
Malicious software (malware)	Technical (External)	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)

References

Alter, S., & Sherer, S. A. (2004). A general, but readily adaptable model of information system risk. *Communications of the Association for Information Systems, 14*(1–28), 1.

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.

Barton, B. F., & Barton, M. S. (1984). User-friendly password methods for computer-mediated information systems. *Computers & Security, 3*(3), 186–195.

Baskerville, R., Park, E. H., & Kim, J. (2014). An emote opportunity model of computer abuse. [article]. *Information Technology & People, 27*(2), 155–181. doi:10.1108/itp-11-2011-0068.

Baur, A. W. (Forthcoming). Harnessing the social web to enhance insights into people's opinions in business, government and public administration. *Information Systems Frontiers*, 1–21.

Bernoff, J., & Schadler, T. (2010). Empowered. *Harvard Business Review, 88*(July–August), 95–101.

Best, R. (1974). An experiment in delphi estimation in marketing decision making. *Journal of Marketing Research, 11*, 448–452.

Bharati, P., Zhang, C., & Chaudhury, A. (2014). Social media assimilation in firms: investigating the roles of absorptive capacity and institutional pressures. *Information Systems Frontiers, 16*(2), 257–272.

Boje, D., & Murninghan, J. (1982). Group confidence pressures in iterative decisions. *Management Science, 28*, 1187–1196.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Chicago: Sage.

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.

Brancheau, J. C., & Wetherbe, J. C. (1987). Key issues in information systems management. *MIS Quarterly, 11*(1), 22.

Brancheau, J. C., & Wetherbe, J. C. (1990). The adoption of spreadsheet software: testing innovation diffusion theory in the context of end-user computing. *Information Systems Research, 1*(2), 115–143.

Brockhoff, K. (2002). The performance of forecasting groups in computer dialogue and face-to-face discussion. In M. Turoff, & H. A. Linestone (Eds.), *The Delphi Method: Techniques and Applications*. Addison-Wesley Publishing Co.

Buckley, J. L. (1974). Family Educational Rights and Privacy Act (FERPA). In U. S. Congress (Ed.), (Vol. 20 U.S.C. § 1232 g; 34 CFR Part 99). Washington, D. C.: United States Congress.

Byrd, S. (2012). Hi fans! Tell us your story!: incorporating a stewardship-based social media strategy to maintain brand reputation during a crisis. *Corporate Communications: An International Journal, 17*(3), 241–254.

Chou, W.-Y. S., Hunt, Y. M., Beckjord, E. B., Moser, R. P., & Hesse, B. W. (2009). Social media use in the United States: implications for health communication. *Journal of Medical Internet Research, 11*(4), e48.

Choudhary, A., Hendrix, W., Lee, K., Palsetia, D., & Liao, W.-K. (2012). Social media evolution of the Egyptian revolution. *Communications of the ACM, 55*(5), 74–80.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). *Enterprise risk management - integrated framework*. New York, NY: Committee of Sponsoring Organizations of the Treadway Commission.

Culnan, M. J., McHugh, P. J., & Zubillaga, J. I. (2010). How large U.S. companies can use twitter and other social media to gain business value. *MIS Quarterly Executive, 9*(4), 243–259.

Dahlander, L., & Piezunka, H. (2014). Open to suggestions: how organizations elicit suggestions through proactive and reactive attention. *Research Policy, 43*, 812–827.

Deans, P. C. (2011). The impact of social media on C-level roles. *MIS Quarterly Executive, 10*(4), 187–200.

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.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. [article]. *Information Systems Journal, 16*(3), 293–314. doi:10.1111/j.1365-2575.2006.00219.x.

Di Gangi, P. M., & Wasko, M. (2009). Steal my idea! Organizational adoption of user innovations from a user innovation community: a case study of Dell IdeaStorm. *Decision Support Systems, 48*(1), 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.

Dickinson, G. W., Leitheiser, R. L., Wetherbe, J. C., & Nechis, M. (1984). Key information systems issues for the 1980's. *MIS Quarterly, 8*(3), 24.

Dijkmans, C., Kerkhof, P., & Beukeboom, C. J. (2015). A stage to engage: social media use and corporate reputation. *Tourism Management, 47*(April), 58–67.

El-Gayar, O. F., & Fritz, B. D. (2010). A web-based multi-perspective decision support system for information security planning. [article]. *Decision Support Systems, 50*(1), 43–54. doi:10.1016/j.dss.2010.07.001.

Gaines-Ross, L. (2013). Get social: a mandate for new CEOs. *MIT Sloan Management Review, 54*(3), 1–5.

Gallaugher, J., & Ransbotham, S. (2010). Social media and customer dialog management at Starbucks. *MIS Quarterly Executive, 9*(4), 197–212.

Goel, S., & Chengalur-Smith, I. (2010). Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems, 19*, 281–295.

Goh, S. H., & Di Gangi, P. M. (2016). A framework for understanding risk perceptions in cooperatives. *The Cooperative Accountant, LXIV*(Summer), Article 2.

Goodhue, D. L., & Straub, D. (1991). Security concerns of system users: a study of perceptions of the adequacy of security. *Information Management, 20*(1), 13–27.

Gramm, P., Leach, J., & Bliley, T. J. Jr. (1999). Gramm-Leach-Bliley Act. In t. U. S. Congress (Ed.), (Vol. Public Law 106–102). Washington, D. C.: United States Congress.

Gray, P., & Hovav, A. (2014). Using scenarios to understand the frontiers of IS. *Information Systems Frontiers, 16*, 337–345.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, 611–642.

Guitierrez, F. J., Ochoa, S. F., Zurita, G., & Baloian, N. (2016). Understanding student participation in undergraduate course communities: a case study. *Information Systems Frontiers, 18*(1), 7–21.

Hanna, R., Rohm, A., & Crittenden, V. L. (2011). We're all connected: the power of the social media ecosystem. *Business Horizons, 54*(3), 265–273.

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

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

Hsu, L., & Lawrence, B. (2015). The role of social media and brand equity during a product recall crisis: a shareholder value perspective. *International Journal of Research in Marketing, 33*(1), 59–77.

Hunton, J. E., Wright, A. M., & Wright, S. (2004). Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems, 18*(2), 7–28.

Ifinedo, P. (2011). An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions. *Journal of Privacy & Security, 7*(1), 25–49.

IT Governance Institute (ITGI) (2005). *COBIT 5*. Rolling Meadows, IL: IT Governance Institute.

Jenkins, C. (2012). Towards 'social' security. *Computer Fraud & Security, 2012*(8), 18–20. doi:10.1016/s1361-3723(12)70084-2.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34*(3), 549–566.

Johnston, A. C., Worrell, J. L., Di Gangi, P. M., & Wasko, M. (2013). Online health communities: an assessment of the influence of participation on patient empowerment outcomes. *Information Technology & People, 26*(2), 213–235.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134.

Kallinikos, J., & Tempini, N. (2014). Patient data as medical facts: social media practices as a foundation for medical knowledge creation. *Information Systems Research, 25*(4), 817–833.

Kane, G. C. (2015a). Can you really let employees loose on social media? *MIT Sloan Management Review, 56*(2), 1–9.

Kane, G. C. (2015b). Enterprise social media: Current capabilities and future possibilities. *MIS Quarterly Executive, 14*(1), 1–16.

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

Kane, G. C., Alavi, M., Labianca, G., & Borgatti, S. P. (2014). What's different about social media networks? A framework and research agenda. *MIS Quarterly, 38*(1), 275–304.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*, 139–154.

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

Kennedy, E., & Kassebaum, N. (1996). Health Insurance Portability and Accountability Act (HIPPA) of 1996. In t. U. S. Congress (Ed.), (Vol. Public Law 104–191). Washington, D. C.: United States Congress.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241–251.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information Management, 41*(5), 597–607.

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

Krasnova, H., Widjaja, T., Buxmann, P., Wenninger, H., & Benbasat, I. (2015). Why following friends can hurt you: an exploratory investigation of the effects of envy on social networking sites among college-age users. *Information Systems Research, 26*(3), 585–605.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*(1), 159–174.

Leidner, D., Koch, H., & Gonzalez, E. (2010). Assimilating generation Y IT new hires into USAA's workforce: the role of an enterprise 2.0 system. *MIS Quarterly Executive, 9*(4), 229–242.

Leonardi, P. M., Huysman, M., & Steinfield, C. (2013). Enterprise social media: definition, history, and prospects for the study of social technologies in organizations. *Journal of Computer-Mediated Communication, 19*(1), 1–19.

Levy, M., Leusner, A., & Wasti, K. (2015). Putting the squeeze on social media: understanding social media regulation, and its associated risks, is key to helping protect the organization from potential harm. *Internal Auditor, 72*(1), 36–42.

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal, 24*(6), 479–502.

Linestone, H. A., & Turoff, M. (2002). *The Delphi method: techniques and applications*. Reading: Addison-Wesley Publishing Co.

Lundmark, L. W., Oh, C., & Verhaal, J. C. (Forthcoming). A little birdie told me: social media, organizational legitimacy, and underpricing in initial public offerings. *Information Systems Frontiers*, 1–16. doi:10.1007/s10796-016-9654-x.

Miller-Merrell, J. (2012). The workplace engagement economy where HR, social, mobile, and tech collide. *Employment Relations Today, 39*(2), 1–9.

Mooney, J. L., Wright Jr., H. R., & Higgins, L. N. (2010). Gen Y's addiction to Web 2.0: problem or strategy? *The Journal of Corporate Accounting & Finance, 22*(1), 63–73.

Ng, B. Y., & Feng, A. E. (2006). An exploratory study on managerial security concerns in technology start-ups. In *10th Pacific Asia Conference on Information Systems, Kuala Lumpur, Malaysia,* pp. 189–196.

Paliwoda, S. (1983). Predicting the future using Delphi. *Management Decision, 21*(1), 31–38.

Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS Quarterly, 24*(1), 81–113.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security, 31*, 221–232.

Sarasohn-Kahn, J. (2008). *The wisdom of patients: Health care meets online social media*. Oakland, CA: California HealthCare Foundation.

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behavior and cyber victimisation: an empirical study of social networking users. *Technological Forecasting and Social Change, 102*(C), 320–330.

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

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: an international delphi study. *Journal of Management Information Systems, 17*(4), 5–35.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.

Tan, T., Ruighaver, T., & Ahmad, A. (2003). Incident handling: Where the need for planning is often not recognised. In *1st Australian Computer, Network & Information Forensics Conference, Perth, Western Australia.*

Tapscott, D. (2008). *Grown up digital: How the net generation is changing your world*. New York: McGraw-Hill.

Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews. *Communications of the Association for Information Systems, 37*(Article 6), 112–137.

Teo, T. S. H., Nishant, R., Goh, M., & Agarwal, S. (2011). Leveraging collaborative technologies to build a knowledge sharing culture at HP analytics. *MIS Quarterly Executive, 10*(1), 1–18.

Tsui, T. C. (2013). Experience from the anti-monopoly law decision in China (Cost and Benefit of Rule of Law). *The Network: Business at Berkeley Law*(April/ May).

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

Viera, A. J., & Garrett, J. M. (2005). Understanding interobserver agreement: the Kappa statistic. *Family Medicine, 37*(5), 360–363.

Vishwanath, A. (2015). Diffusion of deception in social media: social contagion effects and its antecedents. *Information Systems Frontiers, 17*, 1353–1367.

Wakunuma, K. J., & Stahl, B. C. (2014). Tomorrow's ethics and today's response: an investigation into the ways information systems professionals perceive and address emerging ethical issues. *Information Systems Frontiers, 16*, 383–397.

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems, 13*(1), 1–30.

Wesch, M. (2008). An anthropological introduction to YouTube. In U. Library of Congress (Ed.).

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. [article]. *European Journal of Information Systems, 15*(4), 403–414. doi:10.1057/palgrave.ejis.3000592.

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.

Yan, X., Wang, J., & Chau, M. (2015). Customer revist intention to restaurants: evidence from online reviews. *Information Systems Frontiers, 17*, 645–657.

Paul M. Di Gangi is an Associate Professor of Information Systems in the Collat School of Business at the University of Alabama at Birmingham. His research examines the intersection of social networks and organizations with a focus in three areas: 1) user-driven innovation, 2) collective models of organizing, and 3) the implications of information security and social networks on organizations. His research has been published in *Decision Support Systems*, *Information & Organization*, *Information Technology & People*, and *MIS Quarterly Executive*, among others. Paul is a Certified Information Systems Security Professional (CISSP) and teaches courses related to strategic use of social media in business and information security.

Allen C. Johnston is an Associate Professor of Information Systems in the Collat School of Business at the University of Alabama at Birmingham. His research focuses on the areas of behavioral information security, privacy, data loss prevention, and collective security and his research can be found in such outlets as *MIS Quarterly, European Journal of Information Systems,* and *Communications of the ACM*. He currently serves as an associate editor for *European Journal of Information Systems*, *Decision Sciences*, and the *Journal of Information Privacy and Security*, and is a founding member of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13).

James L Worrell, CPA, CISA, CIA is an Associate Professor of Accounting in the Collat School of Business at the University of Alabama at Birmingham. He was a Senior Consultant and founding member of PricewaterhouseCoopers' Security Integration Services practice group and served as IT Internal Audit Manager for a Fortune 500 financial services firm prior to pursuing his doctorate. His research interests include enterprise systems post-implementation issues and IT governance, risk and compliance. He maintains an active consulting portfolio and has published numerous articles in both accounting and information systems peer reviewed outlets.

Samuel C. Thompson is an Assistant Professor of Information Systems in the Collat School of Business at the University of Alabama at Birmingham. He served as an intelligence and security officer in the United States Army during combat operations in Iraq. He has also taught information security courses to corporate and government agency personnel for over a decade. He now teaches and conducts research in information security and privacy.