International Journal of Accounting Information Systems 28 (2018) 31–44

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

journal homepage: www.elsevier.com/locate/accinf

Data availability: Please contact the third author.

Do organizations use a formalized risk management process to address social media risk?

Kristina C. Demek[a,*], Robyn L. Raschke[b], Diane J. Janvrin[c], William N. Dilla[c]

[a] Department of Accounting, College of Business Administration, University of Central Florida, P.O. Box 161400, Orlando, FL 32816, United States
[b] Department of Accounting, Lee Business School, University of Nevada Las Vegas, Las Vegas, NV 89154, United States
[c] Department of Accounting, Debbie and Jerry Ivy College of Business, Iowa State University, Ames, IA 50011, United States

ARTICLE INFO

Keywords:
Social media
Risk management
COSO
Social media policy

ABSTRACT

Social media use within the workplace is widespread; however, little is known about how organizations actually manage social media risk. We use the Committee of Sponsoring Organization's *Enterprise Risk Management – Integrated Framework* (COSO, 2004) to develop a social media risk management model (SM-RMM) that includes four components: (i) social media use, (ii) perceived risk of use, (iii) policy implementation, and (iv) training and technical controls. We utilize the model to examine whether the manner in which organizations address social media risk is consistent with a formalized risk management process. Survey data from 98 risk management, audit, and finance professionals shows that the extent of organizations' social media use increases the perceived risk of social media use. In addition, the effect of the extent of use on the implementation of social media policies is greater for organizations with higher levels of perceived risk of use. Finally, organizations with more extensive social media policies have more extensive training and technical controls. The study's findings indicate that organizations are adopting social media policies and controls in a reactive fashion, as opposed to using a formalized risk management process. This may unduly expose organizations to social media risks. Our model provides a framework for future research on social media risk management.

1. Introduction

Social media is changing how organizations engage externally with customers and other stakeholders, as well as how they interact and collaborate internally with their employees (Kane et al., 2014). Proponents argue that social media use enhances relations with customers and employees and increases the effectiveness and efficiency of an organization's internal operations (Investis, 2015). Indeed, organizational social media use has grown exponentially in recent years (Culnan et al., 2010; Engen, 2012; Tysiac, 2012). Investis' (2015) survey of U.S. companies' corporate social media use reports that 100% of the S&P 100 have at least one corporate social media account, 97% of the largest 500 U.S. companies have LinkedIn accounts, 84% have Twitter accounts, 67% have Facebook accounts, 69% have YouTube video channels, and 39% have Google + pages. Thus, the organizational use of social media is widespread.

While social media use can be beneficial to an organization, it can pose increased risks due to its interactivity, spontaneity, and likelihood of unedited content (Scott and Jacka, 2011). Since social media is a communications tool that resides on an organization's information technology (IT) platform, it has the potential to increase IT security and information leakage risks. Social media use within organizations can also decrease employee productivity and increase reputational risks (Accenture, 2014; Brivot et al., 2017;

* Corresponding author.
E-mail address: Kristina.Demek@ucf.edu (K.C. Demek).

https://doi.org/10.1016/j.accinf.2017.12.004
Received 25 May 2016; Received in revised form 3 December 2017; Accepted 12 December 2017

Hildebrand et al., 2013; ISACA, 2011; Khansa et al., 2017; O'Leary, 2011a; Russell Herder and Ethos Business Law, 2009; Schaupp and Bélanger, 2014; Wilkin and Chenhall, 2010). Each of these risks comes with a potential cost. Indeed, the financial risk of social media mismanagement is a top concern for executives (Deloitte, 2012).

Management, internal auditors, and external assurance providers recognize the importance of addressing social media risk as part of an organization's risk management and internal control program (Brivot et al., 2017; Deloitte, 2009, 2012; Ernst and Young, 2012; ISACA, 2010; Scott and Jacka, 2011). A Protiviti (2015) survey of internal audit directors finds that 56% of respondents' organizations formally assess social media risk. Even so, a gap exists within many organizations between concerns about social media risk and the existence of formal social media risk management strategies that are applied throughout the organization (Deans, 2011; Geyer and Krumay, 2015; Larcker et al., 2012; Scott and Jacka, 2011). Illustrating this gap, a survey of senior level executives from U.S. companies reports that 84% of respondents have concerns about the implications of social media, yet only 18% are aware of their organizations performing risk assessments (Grant Thornton, 2013). This, in turn, suggests that only a minority of organizations take a *proactive* approach to social media risk management through a formalized risk assessment process. Other organizations may be following a *reactive* approach in which they adopt social media policies and controls without conducting formalized risk assessments. Consequently, it is important to understand the extent to which organizations are taking a reactive approach to managing social media risks, since the failure to adequately manage these risks can have a detrimental effect on organizational profitability and ultimately, on shareholder wealth (Accenture, 2014; IRM, 2002; Scott and Jacka, 2011). In order to address this concern, this paper addresses the question, "Are organizations taking a reactive approach to managing their social media risks?"

In order to examine whether organizations are taking a proactive or reactive approach to managing social media risks, we use the Committee of Sponsoring Organization's *Enterprise Risk Management – Integrated Framework* (ERM-IF) (COSO, 2004) to develop a social media risk management model (SM-RMM henceforth). We identify four components of social media risk management: (i) social media use, (ii) perceived risk of use, (iii) policy implementation, and (iv) training and technical controls. Social media use addresses how organizations employ social media both externally and internally. Given that the SM-RMM focuses on the use of social media by an organization and its employees, it specifically addresses social media use that an organization can control. The perceived risk of use involves how organizations view IT security, information leakage, employee productivity, and reputational risks that may arise because of social media use. Policy implementation refers to the existence of policies designed to manage social media risks. Finally, training and technical controls refer to the development and implementation of social media training programs and to procedures designed to support social media risk management policies.

While the SM-RMM flows from the ERM-IF and provides a *prescriptive*, proactive model for how organizations *should* manage social media risk, the model also allows for the examination of social media risk management from a *descriptive*, reactive viewpoint. From a proactive standpoint, the SM-RMM indicates that organizations should first formally assess the risks associated with social media use, then implement social media policies and controls based on these risk assessments. This sequence is consistent with the ERM-IF and suggests that the implementation of social media policies and controls flows from a formalized risk assessment process. Alternatively, organizations may follow a reactive approach in which they adopt social media policies and controls, without first conducting a formalized risk assessment of social media use (Larcker et al., 2012; Scott and Jacka, 2011). This may occur since social media use is pervasive across many areas of an organization, social media technologies are easy to adopt, and social media applications often are adopted without a formalized implementation plan (Aggarwal and Singh, 2013; Baird and Parasnis, 2011; Brivot et al., 2017; Heinrichs et al., 2011; Leonardi, 2014). Further, research suggests that organizations have insufficient risk management procedures at the individual systems level (Arena et al., 2010; Hayne and Free, 2014; Power, 2007, 2009). These factors indicate that organizations may be taking a reactive approach to social media risk management and adopting social media policies on an ad hoc basis. Under such an approach, the extent to which organizations implement social media policies and controls is likely to be a function of both the extent of social media use and the perceived risk of use. While the extent of social media use will primarily drive the extent of policy implementation, the perceived risk of use will have a moderating effect on policy and control implementation. Specifically, a reactive approach to social media risk management suggests that the extent of social media use on the adoption of social media policies and controls is likely to be greater for organizations with higher levels of perceived risk of use.

To examine our research question, we develop a set of hypotheses which tests whether organizations are taking a reactive approach to managing their social media risks. We test these hypotheses using responses from 98 corporate risk management, audit, and finance professionals. Consistent with our predictions, we find that the extent of social media use increases the perceived risk of use. Next, we find that the perceived risk of use moderates the effect of social media use on policy implementation, such that the effect of social media use on policy implementation is greater for organizations with higher levels of perceived risk of use. Finally, we find that social media policy implementation increases the extent to which organizations implement training and technical controls related to social media.

In contrast to the reactive view reflected by our hypotheses, the proactive view of the SM-RMM suggests that if organizations are following a formal risk assessment process, the perceived risk of use should mediate the relation between social media use and policy implementation, as opposed to the moderating effect indicated by the reactive view. Supplemental analysis shows that the perceived risk of use does *not* mediate the relation between social media use and policy implementation. Therefore, our hypotheses testing and supplemental analysis support the conjecture that organizations are following a reactive approach to social media risk management. These results are consistent with observations from the practitioner literature (Scott and Jacka, 2011), and with prior research which documents instances where organizations have insufficiently adopted risk management strategies across all their systems (Arena et al., 2010; Hayne and Free, 2014; Power, 2007, 2009).

This paper contributes to both academic research and to practice. The academic literature has only begun to address organizational risks associated with social media use (Arnaboldi et al., 2017; Geyer and Krumay, 2015; He, 2012; O'Leary, 2011a, 2011b;

Rose, 2011). These studies, however, only describe the risk of social media use, without providing empirical evidence with regard to social media risk management practices. This paper develops a model of social media risk management, which includes four components that researchers can use as a framework to develop additional research in these areas: social media use, perceived risk of use, policy implementation, and training and technical controls.

This study should also be of interest to practitioners, since the results suggest that organizations are managing social media risks on a reactive basis, as opposed to following a proactive, formalized risk management process. Understanding the gap between normative best practices and actual policy in this area is important, as senior managers and boards of directors are increasingly concerned about social media oversight (Grant Thornton, 2013; KPMG, 2013; Larcker et al., 2012). Indeed, failure to appropriately manage social media risk can lead to unintended costs that outweigh the benefits to be obtained from organizational social media use.

The next section discusses background literature related to the use of social media in organizations, how organizations may use a formalized risk management process to address social media risks, and the use of the ERM-IF to develop the SM-RMM. The third section of the paper presents the study's hypotheses. The fourth and fifth sections of the paper describe the research method and present the results, respectively. The final section concludes the paper.

2. Background

2.1. Social media in organizations

Social media can be described as “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content” (Kaplan and Haenlein, 2010, 61). Whereas Web 1.0 technologies facilitated largely one-way information flows with limited opportunities for user engagement and interaction, Web 2.0 technologies allow for the active creation of content by their users or members. Social media tools include social networking (e.g., Facebook and LinkedIn), blogs (e.g., Blogger and WordPress), reviews and rating services (e.g., Amazon, Trip Advisor, and Yelp), photo and video sharing (e.g., Flickr and YouTube), document and content sharing (e.g., Dropbox and Google Docs), podcasts (e.g., iTunes), and knowledge sharing (e.g., Wikipedia) (Scott and Jacka, 2011). Hence, social media is much more than a one-way information transfer *from* organizations, as it increasingly becomes a social and communal two-way communication platform *between* organizations and their stakeholders (Preece and Shneiderman, 2009). In addition, social media technology allows managers to easily engage and share in this information environment (Ravichandran and Liu, 2011).

Given that social media is complex and touches many areas of an organization, and the content of social media is more likely to be spontaneous and unedited compared to other types of organizational communication, it engenders risks not encountered in other forms of data transmission (Bennett, 2008). Specifically, social media risks can stem from the organization's use of social media, from employees' use of social media, from external sources to the organization, or from a combination of these sources. Below, we identify and describe four broad categories of risk associated with organizational social media use: IT security, information leakage, employee productivity, and reputational.

Social media poses an IT security risk through the potential introduction of viruses, spam, and malware (van Zyl, 2009). In particular, employees using social media on the organization's devices might be enticed through social engineering techniques to disclose corporate login and password information (Ernst and Young, 2012, 2014b; Langheinrich and Karjoth, 2010).

Social media use increases the risk of intentional or unintentional leakage of confidential information, such as employee or customer data or proprietary intellectual property. Information leakage may lead to regulatory, compliance, or legal issues if employees disclose confidential organizational information via posting comments on their personal social media pages (Ernst and Young, 2014b; Greene and O'Brien, 2013; Langheinrich and Karjoth, 2010). For example, in June 2012, Netflix CEO W. Reed Hastings announced on his personal Facebook page that the company had just streamed more than 1 billion hours of Internet Video (ElBoghdady, 2013; Katz and McIntosh, 2013). This announcement generated a warning from the Securities and Exchange Commission (SEC) that future similar incidents would be viewed as violations of Regulation Fair Disclosure (FD), since Netflix did not share this milestone in a news release or other public channel such as the company's website or official Facebook page (SEC, 2013). Ultimately, the SEC announced that companies can use social media to announce organizational information in compliance with Regulation FD, as long as investors have been previously alerted about which social media tool will be used to communicate such information (SEC, 2013). Thus, the SEC guidance poses a substantial compliance risk for companies that choose to disclose financial and operational information through social media.

Additionally, social media use may threaten employee productivity. Social media presents employees with the challenge of navigating the boundaries between their personal and professional identities (Ollier-Malaterre et al., 2013). Excessive employee social media use for personal purposes during working hours may result in productivity losses to organizations and misuse of resources (Ernst and Young, 2012; Field and Chelliah, 2012; Khansa et al., 2017). Some IT practitioners, however, have challenged this view, citing survey results where 46% of respondents report that using social media at work increases productivity and 30% state that their organizations underestimate the value of social media (Microsoft, 2013; Smith, 2013). Thus, it is not clear whether social media use decreases employee productivity, or if employees can overcome this challenge and employ social media to increase productivity.

Finally, damage to an organization's reputation may occur when employees post negative comments on social media about its products or policies (Brivot et al., 2017; O'Leary, 2011a). In addition to reputational risk concerns that can arise from negative, embarrassing, or incriminating employee comments, hackers may infiltrate an organization's social media accounts and post false or misleading information (Castillo et al., 2011). Brivot et al. (2017) further note that controlling reputational risk is difficult as there are multiple, conflicting viewpoints as to how social media risk should be controlled, if at all. However, reputational risk that arises

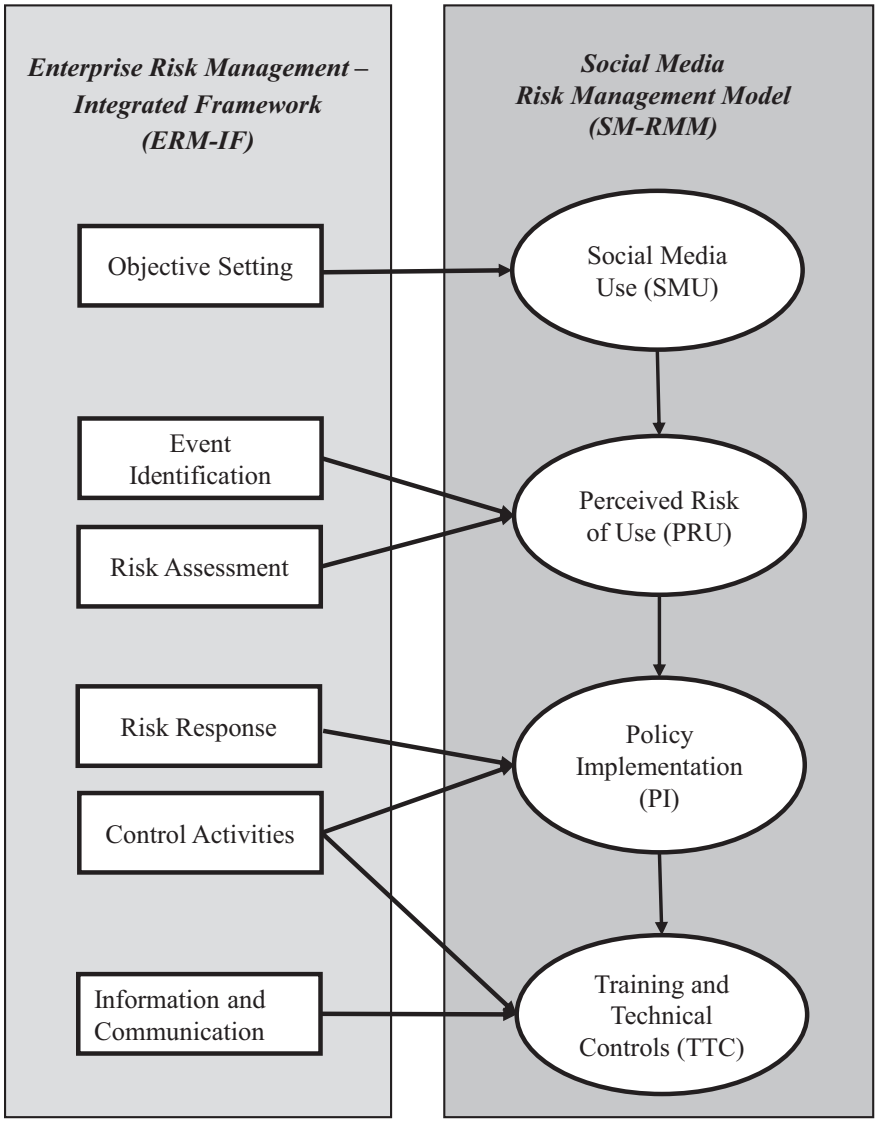

Fig. 1. Social media risk management model (SM-RMM).

from social media use by customers or other parties outside the organization is outside the scope of the social media risk management model developed in the next section.

2.2. Using COSO's ERM-IF to develop a social media risk management model

The ERM-IF has become a "best practice" standard for organizations to manage risks (Arena et al., 2010; Hayne and Free, 2014; Power, 2007). This framework addresses an organization's objectives across strategic, operations, reporting, and compliance categories (COSO, 2004). It has been applied to manage cloud computing risks (Chan et al., 2012) and IT security risks related to online transactions (Galligan and Rau, 2015). These prior IT-related applications indicate that the ERM-IF is an appropriate framework for conceptualizing the management of risks associated with social media use within organizations.

The SM-RMM addresses how social media use by organizations and their employees influences the perceived risk associated with social media use. In addition, it addresses the influence of social media use and perceived risk of use on the implementation of social media policies, training, and technical controls. To develop the SM-RMM, we incorporate six of the ERM-IF components: objective setting, event identification, risk assessment, risk response, control activities, and information and communication. As shown in Fig. 1, we apply these six ERM-IF components to establish four components of the SM-RMM: social media use, perceived risk of use, policy implementation, and training and technical controls.

The *Objective Setting* component of the ERM-IF indicates that before an organization can begin to conduct a formal risk assessment and identify the risks and opportunities associated with one of its systems, it needs to understand the objectives of using the system

within the organization. Objective Setting maps onto the *Social Media Use* component of the SM-RMM, given that organizations use social media to achieve specific goals, such as improving communications with customers, increasing sales leads, developing and maintaining an organization's brand, and effectively communicating with employees.

The *Event Identification* component of the ERM-IF refers to the act of identifying external and internal events which affect achievement of an organization's objectives. These events can serve either as risks or as opportunities. Once an organization identifies its risks, the *Risk Assessment* component involves the analysis of the likelihood and magnitude of each risk. This analysis provides a basis for determining how the organization should manage each identified risk. The Event Identification and Risk Assessment components of the ERM-IF map onto the *Perceived Risk of Use* component of the SM-RMM, given that these ERM-IF components are directly related to identifying an organization's perceived risk of social media use.

The *Risk Response* and *Control Activities* components of the ERM-IF relate to how an organization manages its risks. In the *Risk Response* component, management develops a set of actions to reduce risks, in line with the organization's risk tolerance. The *Control Activities* component of the ERM-IF refers to the policies and procedures that an organization establishes and implements to ensure it effectively implements appropriate risk responses. Both *Risk Response* and *Control Activities* map onto the *Policy Implementation* component of the SM-RMM.

Finally, two components of the ERM-IF map onto the *Training and Technical Controls* component. Some of the *Control Activities* that an organization may elect to implement are technical controls, such as procedures that are designed to identify, block, or prevent potential information security incidents related to social media use (ISACA, 2010). Further, an organization needs to conduct training in order to ensure that employees follow established policies and procedures. *Information and Communication* maps onto the *Training and Technical Controls* component of the SM-RMM, since training conveys information to employees regarding the proper implementation of the organization's social media risk management policies.

Two remaining components of the ERM-IF are outside the scope of the SM-RMM. The *Internal Environment* is the tone of the organization, which helps establish the risk management philosophy and risk appetite of the organization. Although the tone of the organization is an integral part of effective risk management, it is a holistic component, which applies to the organization's overall risk management philosophy. Since the SM-RMM relates to the risk management of a specific system, it does not incorporate the Internal Environment component of the ERM-IF. The *Monitoring* component of the ERM-IF involves ongoing evaluations of the risk management process, with modifications made as necessary. The SM-RMM does not explicitly incorporate this component, since its focus is on the process of assessing and responding to social media risk, as opposed to the evolution of risk management in response to monitoring activities.

3. Hypothesis development

The SM-RMM depicted in Fig. 1 indicates that social media policy implementation is likely a function of both an organization's social media use and perceived risk of use. While the apparent association between social media use and policy implementation is positive, prior academic and practice research suggests this relation may also be dependent on whether an organization takes a proactive or reactive approach to social media risk management (Larcker et al., 2012; Scott and Jacka, 2011). Due to the nature of social media use, we argue that organizations are taking a reactive approach to social media risk management. Overall, this suggests that perceived risk of use will moderate the effect of social media use on policy implementation, as shown in the research model depicted in Fig. 2. Specifically, the effect of social media use on policy implementation will be greater for organizations with higher levels of perceived risk of use.

The following sections develop the hypotheses indicated by our research model, which allow us to address whether organizations are taking a reactive approach to managing their social media risk.

3.1. The influence of social media use on perceived risk of use

The Social Media Use component of the SM-RMM indicates that in order for organizations to manage social media risk, they first need to identify how they implement and use social media across all areas. This flows from the perspective of the ERM-IF, where the purpose of the Objective Setting component is to identify how organizations and their employees use social media externally and internally.

Externally, organizations use social media to attract customers and communicate with investors and the public (Katz and McIntosh, 2013; Michaelidou et al., 2011). Organizations use social media to increase efficiencies within the supply chain, monitor the market and competition, and communicate with investors and analysts (O'Leary, 2011b; Trinkle et al., 2015). In addition, organizations use social media as a recruiting tool to attract new employees and prescreen potential future employees (Greenwald, 2010). Further, organizations use social media to build brand reputation, increase sales, and obtain consumer feedback in order to improve products and customer service (Ernst and Young, 2014a; Eschenbrenner et al., 2015; Katz and McIntosh, 2013; KPMG, 2013; Schaupp and Bélanger, 2014). Internally, organizations use social media as an interactive internal communication, collaboration and knowledge-sharing tool, to brainstorm about new product development, and obtain employee feedback about the organization (Ernst and Young, 2014a; Eschenbrenner et al., 2015; Katz and McIntosh, 2013; KPMG, 2013; Perry, 2009; Schaupp and Bélanger, 2014). Managers perceive that these external and internal uses of social media add value to the organization by increasing sales contacts, reducing marketing costs, improving customer service, and increasing staff productivity (Schaupp and Bélanger, 2014).

The Perceived Risk of Use component of the SM-RMM indicates that once an organization identifies how it uses social media, it needs to identify and assess risks, as indicated by the ERM-IF's Event Identification and Risk Assessment components. Improperly

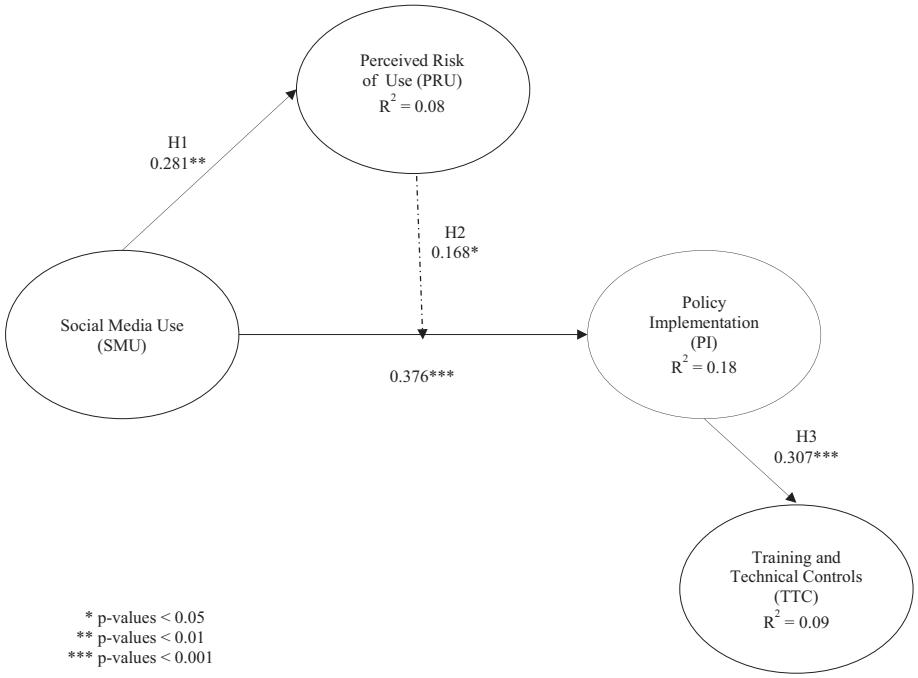

Fig. 2. Research model and PLS results.

addressed social media risks can lead to a decline in customer confidence, reduce market share, and negatively impact an organization's reputation (Brivot et al., 2017; Ernst and Young, 2014b). Normatively, organizations should assess and balance opportunities and risks when deciding on a social media strategy (Haimes, 2012; ISACA, 2010; Scott and Jacka, 2011). However, organizations may only become aware of social media risks as their extent of use increases (Scott and Jacka, 2011). In either case, the more that organizations use social media, the more managers will perceive that their organizations are exposed to IT security, information leakage, employee productivity, and reputational risks. This leads to the following hypothesis:

H1. Social media use will increase the perceived risk of use.

3.2. The moderating role of perceived risk of use

Implementing social media use policies within an organization is an important step toward managing social media risk (Scott and Jacka, 2011). Organizations may rely on existing policies or establish new policies to guide employee behavior with respect to social media (Ernst and Young, 2012; Haimes, 2012). These policies may include specific guidelines, such as specifying what employees can and cannot say online regarding organizational information and activities. Alternately, organizations may provide general guidelines and allow employees discretion when posting comments and opinions on social media (Ernst and Young, 2012). Thus, as organizations become more aware of social media risk, they are more likely to establish policies regarding social media use. However, the level of policy implementation is likely to depend on the organization's perceived risk of use.

A reactive approach to managing social media risk involves reacting to this risk on an ad hoc basis as the extent of organizational social media use increases. In this approach, organizations may implement social media tools without a formalized risk management process, since social media does not require significant new infrastructure or investment (ISACA, 2010). In addition, since social media tools require relatively little technical expertise to adopt, they may not be subject to the same risk management procedures as other IT applications (Scott and Jacka, 2011). For example, marketing executives may implement social media strategies designed to increase sales without considering the risk implications for other segments of the organization's operations (Ernst and Young, 2014b). Such an approach is consistent with the concern expressed by Larcker et al. (2012) that organizations may implement social media applications without adequately considering the impact of social media on corporate strategy development and risk management programs.

Under this reactive approach, managers attempt to address social media risk only after becoming aware of the extent of organizational social media use and the associated risks. The normative approach presented in the ERM-IF indicates that an organization can respond to an identified risk by avoiding it, accepting it as is, sharing it, or reducing the risk (COSO, 2004). Avoiding social media use is not a risk management option under the reactive approach given that, in most cases, it will be difficult for the organization to stop using social media once it has started doing so. However, the organization still has the options of accepting, sharing, or reducing social media use. For example, if an organization perceives the risk of employees using social media to be minimal, it might accept the risk and allow employees to access personal social media accounts from their work computers. Further, many social media

implementation experts argue that organizations should not attempt to control reputation risks, but rather, should consider social media "an invitation to participate in authentic discussions with stakeholders" (Brivot et al., 2017, 801). Alternatively, an organization may choose to share the risks associated with social media use by contracting with third-party organizations to monitor social media or by purchasing new cybersecurity insurance policies (Constantin, 2014). Finally, an organization can reduce social media risk occurring by developing appropriate policies, controls, and training.

Thus, while the extent of social media use will directly influence social media policy implementation, the organization's perceived risk of social media use will moderate this relationship. Specifically, as the organization's perceived risk of social media use increases, the influence of social media use on policy implementation will increase. This indicates the following hypothesis:

H2. Perceived risk of use will moderate the influence of social media use on policy implementation.

3.3. The influence of policy implementation on training and technical controls

The Training and Technical Controls component of the SM-RMM framework addresses the implementation of training and technical controls designed to reduce social media risk (Haimes, 2012; ISACA, 2010; Russell Herder and Ethos Business Law, 2009; Scott and Jacka, 2011). Training regarding social media policies is important, given that many employees are not aware of the existence of such policies within their organization. For example, 58% of respondents to a Deloitte (2009) Ethics and Workplace Survey indicated that either their organization had no social media policy or they were not aware of an existing policy. In addition, 49% of survey respondents indicated that even if there were a policy, it would not change their social media use behavior (Deloitte, 2009). Thus, even if employees are aware of social media policies, they are likely to ignore such policies unless given appropriate training.

Training on social media policies not only provides employees the opportunity to learn about existing policies but also helps them understand the risks associated with social media use (Scott and Jacka, 2011). Best practices suggest that training should occur on a regular basis and focus on the benefits and opportunities of social media use. In addition, training should inform employees about social media-related risks such as social engineering to gain access to sensitive information, software exploits through insecure applications, and other threats to data privacy (ISACA, 2010).

Social media technical controls utilize a combination of web content filtering, antivirus software, and operating system security (ISACA, 2010). Technical monitoring controls assist in policy enforcement by identifying cases where employees have been violating social media policies. In addition, such controls may facilitate blocking, preventing, or identifying potential incidents in cases where relying on policy compliance may not be sufficient to manage social media risk. Indeed, best practices for social media adoption suggest a need for organizations to develop related training and technical controls after establishing social media policies (Bockius and Selby, 2011). This leads to the following hypothesis:

H3. Social media policy implementation will increase the extent to which training and technical controls are present.

4. Research methodology

4.1. Respondents

Survey data were collected from risk management, audit, and finance professionals attending an enterprise risk forum in the Pacific Northwest sponsored by the Risk Management Society (RIMS), Institute of Internal Auditors (IIA), and Financial Executives International (FEI). Risk management, audit, and finance professionals are an appropriate population for this study as these individuals are most likely responsible for social media risk management and governance (Scott and Jacka, 2011; Wilkin and Chenhall, 2010). Two co-authors attended the conference and collected data from the attendees. Survey respondents received a $5 gift card for a national chain of coffee shops.

The sample consists of 103 individuals out of 243 attendees, for a response rate of 42%. We dropped four participants from the sample because they answered no to the question "Does your organization have an established social media policy?" but yes to at least one question regarding "What specific areas does your social media policy address?". Finally, one participant was removed from the sample because he/she indicated that he/she was a full-time student. The results presented below are based on the remaining 98 sample respondents.

Table 1 presents demographic data on the respondent responses used in the analysis. Of the 98 respondents, 37 (37.8%) were male, 52 (53.1%) female, and 9 (9.1%) did not answer. Eighty-six respondents (87.8%) had over 10 years of work experience. Thirty-seven respondents (37.8%) are employed at publicly held organizations, 36 (36.7%) at non-publicly traded organizations, and 24 (24.5%) at government or nonprofit organizations. Fifty-four (55.1%) respondents were from organizations with less than 10,000 employees and 35 respondents (35.7%) were from organizations with more than 10,000 employees.

4.2. Survey instrument and constructs

The survey instrument consisted of two parts. The first part gathered demographic information about the respondents and their organizations' use of social media. The second part captured measures of the research model constructs. The survey was developed by the researchers based on a review of prior practitioner research (COSO, 2013; ISACA, 2010; Larcker et al., 2012; Scott and Jacka,

Table 1
Sample demographics.

Category	Frequency (n = 98)	Percentage
Gender		
Male	37	37.8%
Female	52	53.1%
Not answered	9	9.1%
Age		
26–35	19	19.4%
36–45	32	32.7%
46–55	30	30.6%
> 55	16	16.3%
Not answered	1	1.0%
Experience		
< 10 years	11	10.7%
11–19 years	32	32.0%
20–29 years	28	29.1%
30 or more	26	27.2%
Not answered	1	1.0%
Industry		
Retail	16	16.3%
Insurance	13	13.3%
Banking	8	8.2%
Healthcare	7	7.1%
Telecommunications	7	7.1%
Consulting	5	5.1%
All other	42	42.9%
Organizational structure		
Publicly traded	37	37.8%
Not publicly traded	36	36.7%
Government/Nonprofit	24	24.5%
Not answered	1	1.0%
Organizational Size		
< 20 Employees	2	2.0%
20–99 Employees	2	2.0%
100–499 Employees	11	11.2%
500–999 Employees	11	11.2%
1000–4999 Employees	26	26.5%
5000–9999 Employees	2	2.0%
≥ 10,000 Employees	35	35.7%
Not answered	9	9.2%

2011), and then revised after receiving feedback from the risk management organization. As shown in Fig. 2, the research model includes four constructs corresponding to the components of the SM-RMM: social media use, perceived risk of use, policy implementation, and training and technical controls. Table 2 presents the items used to assess each construct. Questions that assessed social media use, perceived risk of use, and training and technical controls constructs used a five-point Likert-type scale, where "1" represents strongly disagree and "5" represents strongly agree. Questions about policy implementation required yes or no answers.

Social media use (SMU) is a formative construct which represents respondents' perceptions regarding how their organization is using social media externally with customers and internally with employees (Russell Herder and Ethos Business Law, 2009). Measures of social media *external* use address the use of social media to communicate with customers, increase sales, develop and maintain the organization's brand, and recruit and communicate with new employees. *Internal* social media use addresses developing new products. The analysis treats SMU as a formative construct, since changes in the various indicators of SMU are assumed to determine changes in the value of this construct (Hair et al., 2011), and these indicators are not necessarily correlated.

The perceived risk of use (PRU) is a reflective construct depicting respondents' perceptions of their organization's current risk concerns regarding social media use (Ernst and Young, 2012; ISACA, 2010; Russell Herder and Ethos Business Law, 2009). One measure addresses IT security risk, two measures address information leakage (i.e., intellectual property and litigation), and one measure addresses employee productivity risk. Two measures address reputational risk (i.e., the organization's overall reputation and the reputation of its products). The analysis treats PRU as a reflective construct, since the values of individual measures are assumed to be driven by respondents' overall perceptions of the risk associated with social media use, and the individual measures are expected to be correlated (Hair et al., 2011).

Policy implementation (PI) reflects the degree to which an organization has implemented specific policies regarding social media use. It is a second-order reflective construct, with three underlying first-order constructs that address policies on: (i) employees' personal use of social media, (ii) employees' work-related use of social media, and (iii) human resources-related policies (ISACA, 2010; Scott and Jacka, 2011). Two measures assess each underlying construct.

Finally, social media training and technical controls (TTC) is a single construct, with two reflective measures. The first measure

Table 2
Constructs.

Social Media Use (SMU)[a]
Our organization uses social media to:
SMU1 Improve communications with customers.
SMU2 Increase sales leads and sales
SMU3 Develop and maintain our brand.
SMU4 Develop new products.
SMU5 Recruit new employees.
SMU6 Communicate with current employees.
Perceived Risk of Use (PRU)[a]
Our organization is concerned:
PRU1 That the use of social media can damage our reputation.
PRU2 That our products/services will be portrayed in a negative light by consumers using social media.[c]
PRU3 That viruses and malware may be introduced into the corporate network because of employee use of social media.
PRU4 About intellectual property leakage due to social media use.
PRU5 About litigation due to social media use
PRU6[c] That employees' personal use of social media at work negatively impacts productivity.
Social Media Policy Implementation (PI)[b]
Does your organization have a specific policy that addresses:
Personal Use (PI-P)
PI-P1 Employee personal use of social media in the workplace?
PI-P2 Employee personal use of social media outside the workplace?
Workplace Use (PI-W)
PI-W1 Employee use of social media for workplace purposes on personally owned devices?
PI-W2 Employee use of social media for workplace purposes in the workplace?
Human Resources Use (PI-HR)
PI-HR1 Human Resource's ability to use social media as a pre-employment screening tool?
PI-HR2 Human Resource's ability to take disciplinary action against employees for their use of social media?
Social Media Training and Technical Controls (TTC)[a]
TTC1 Our organization has adequate training in place for employees to ensure that they understand appropriate uses of social media.
TTC2 Our organization has adequate technical controls to support social media policies.

[a] Respondents indicated the level of agreement/disagreement with each statement on a 5 point scale where 1 = strongly disagree and 5 = strongly agree.
[b] Respondents provided "yes/no" answers to these questions.
[c] Dropped due to low loading on construct.

reflects the extent to which an organization has adequate training on social media use for employees and the second measure reflects the extent to which an organization has technical controls to address social media use (ISACA, 2010; Scott and Jacka, 2011). Table 3 presents construct descriptive statistics and correlations.

5. Analysis and results

5.1. Method of analysis

We test the research model in Fig. 2 using the WarpPLS 5.0 program (Kock, 2010, 2015). WarpPLS allows for the use of dichotomous measures such as those used to assess PI. Since it uses a bootstrapping technique to model parameters and *p*-values, measures do not need to meet parametric expectations (Kock, 2014a).

Table 3
Construct descriptive statistics and correlations.

Construct (n = 98)	Mean	Std. Dev	CR	AVE	SMU	PRU	PI	TTC
Social media use (SMU)	3.604	1.052	0.860	0.509	**0.714**			
Perceived risk of use (PRU)	3.754	1.034	0.869	0.624	0.238*	**0.791**		
Social media policy implementation (PI-2nd order)	0.760	0.388	0.744	0.529	0.384***	0.334***	**0.727**	
Social media training & technical controls (TTC)	3.019	1.106	0.884	0.792	0.370***	0.315**	0.255**	**0.887**

Notes: CR: Composite Reliability.
AVE: Average Variance Extracted.
Remainder of table shows correlations among constructs, with bolded items on the diagonal representing the square roots of AVEs.
* Denotes correlation p-values of 0.05.
** Denotes correlation p-values of 0.01.
*** Denotes correlation p-values of 0.001.

Table 4
Item loadings and cross-loadings.

Construct (n = 98)	Indicator	Perceived risk of use (PRU)	Policy implementation (PI)	Training and technical controls (TTC)
Perceived risk of use (PRU)	PRU1	**0.749**	0.288	− 0.176
	PRU3	**0.813**	− 0.007	− 0.155
	PRU4	**0.781**	− 0.277	0.194
	PRU5	**0.815**	0.008	0.130
Policy implementation (PI)*	PI-P	− 0.031	**0.743**	− 0.102
	PI-W	0.212	**0.677**	0.065
	PI-HR	− 0.176	**0.684**	0.047
Training and technical controls (TTC)	TTC1	0.018	− 0.112	**0.886**
	TTC2	− 0.018	0.112	**0.886**

Factor loadings are shown in bold.
* 2nd Order Reflective - Latent Variable Scores.

5.2. Convergent and discriminant validity

As shown in Table 3, the average variance extracted (AVE) for each reflective construct exceeds 0.50, and the composite reliability (CR) exceeds 0.70 for all constructs. The AVE and CR measures, therefore, indicate that the reflective constructs possess convergent validity (Fornell and Larcker, 1981; Hair et al., 2012). As shown in Table 4, the factor loadings for all first-order reflective item indicators (PRU and TTC) are greater than 0.70, and the loadings are all greater than the related cross-loadings. This provides additional support for convergent validity. Indicators PRU2 (products and services portrayed in a negative light by customers) and PRU6 (negative impacts of personal social media use at work) were not included in the model, since an initial analysis showed loadings less than 0.70. The fact that PRU2 did not load on the PRU construct indicates that respondents may have perceived this indicator to be different from the other indicators of social media risk, in that it relates to a risk factor that cannot be addressed by organizational social media policies and controls. The fact that PRU6 did not load on the PRU construct indicates that respondents may have perceived that social media use in the workplace does not pose a risk, consistent with the views of some IT practitioners (Microsoft, 2013; Smith, 2013).

To assess discriminant validity, the square-root of the average variance extracted (AVE) for each latent variable was compared with the related inter-construct correlations (Hair et al., 2012). As shown in Table 3, the square root of the AVE for each latent variable is greater than the variable's inter-construct correlations, thus indicating discriminant validity.

5.3. Formative construct validity

There are two commonly used measures of formative construct validity, variance inflation factors (VIF) and outer weights for formative measures. Table 5 presents these measures for the SMU construct. VIFs indicate whether collinearity exists among formative construct measures. All VIFs for the construct measures are less than the commonly accepted threshold of 3.30 (Kock and Lynn, 2012), indicating that collinearity is not present among these measures. All of the outer weights for the construct measures are significantly different from zero, indicating that the measures are valid indicators of the formative constructs.

5.4. Test of lateral collinearity

We performed a test of lateral collinearity on the constructs, since collinearity may cause distorting effects in the strength of the assessed relationships (Kock and Lynn, 2012). The collinearity test also serves as an indicator of common methods bias. As shown in Table 6, all the construct VIFs are below the recommended threshold of 3.30. Therefore, the threat of lateral collinearity does not exist in the data.

5.5. Hypotheses tests

Fig. 2 depicts the results of the structural model analysis, which predicts that organizations are taking a reactive approach to

Table 5
Formative construct validity for SMU.

Indicator (n = 98)	Variance inflation factor (VIF)	Outer weight	p-value
SMU1	1.955	0.235	0.007
SMU2	1.867	0.252	0.004
SMU3	2.219	0.274	0.002
SMU4	1.455	0.227	0.009
SMU5	1.454	0.193	0.023
SMU6	1.533	0.212	0.014

Table 6
Variance inflation factors (VIF) for test of lateral collinearity (n = 98).

Social media use	Perceived risk of use	Policy implementation	Training and technical controls
(SMU)	(PRU)	(PI)	(TTC)
1.303	1.209	1.317	1.278

managing their social media risks. The Tenenhaus goodness of fit statistic for this model is 0.260, indicating that the model has moderate explanatory power (Kock, 2015).[1] H1 predicts that social media use will increase the perceived risk of use. The path coefficient from SMU to PRU (0.281) is positive and significant ($p < 0.01$), confirming this hypothesis. H2 predicts that a higher perceived risk of use will moderate the influence of social media use on policy implementation. The path coefficient from SMU to PI (0.376) is positive and significant ($p < 0.001$), indicating that the extent of social media use increases the extent of social media policy implementation. The moderating path from PRU is positive (0.168) and significant ($p < 0.05$), thus confirming H2. H3 predicts that social media policy implementation will increase the extent to which training and technical controls are present. The path from PI to TTC (0.307) is significant ($p < 0.001$), confirming this hypothesis. Thus, the results of the model in Fig. 2 are consistent with the idea that organizations are taking a reactive approach to social media risk management.

5.6. Supplemental analysis

An alternative to the *reactive* approach is that organizations are actually taking a formalized, *proactive* approach to assessing and managing social media risks. Under risk management best practices, which are the basis for the proactive approach, organizations should first conduct a formal risk assessment that identifies and assesses social media risks, and then determine appropriate responses to these risks (COSO, 2004; Ernst and Young, 2012). This suggests that perceived risk should mediate the influence of social media use on policy implementation. To test for mediation, we used WarpPLS to fit the model depicted in Fig. 3. The Tenenhaus goodness of fit statistic for this model is 0.284, indicating that the model has moderate explanatory power (Kock, 2015). The model also provides an estimate of the significance of the indirect effects of social media use on policy implementation (Kock, 2014b, 2015). This approach follows Preacher and Hayes' (2004, 2008) recommendation of using a bootstrapping technique to estimate the significance of indirect effects.

As shown in Fig. 3, the direct paths from SMU to PRU and from PRU to PI are both significant ($p < 0.01$). However, the indirect path from SMU to PI through PRU (0.077) is not significant ($p > 0.10$). Further, the direct path from SMU to PI (0.319) remains significant ($p < 0.001$), even when including PRU in the model as a mediator. Therefore, the lack of a mediating effect is inconsistent with organizations taking a normative, proactive approach to managing social media risk. The lack of a significant mediation model, in conjunction with a significant moderation model, suggests that organizations are taking a reactive approach to social media risk management and implementing social media policies on an ad hoc basis. Such an approach indicates that organizations are not using a formalized risk management process per best practices indicated by the ERM-IF. This may occur because management lacks an understanding of the nature and extent of their organization's social media use or because they may have not fully considered the risks associated with social media use. In either case, it is possible that organizations will incur unintended costs due to ineffective risk management that outweigh the benefits to be obtained from organizational social media use. This possibility is consistent with the concern expressed by Larcker et al. (2012) that organizations may implement social media applications without adequately considering the impact of social media on corporate strategy development and risk management programs.

6. Conclusions

Social media use has emerged in recent years as an important way for organizations to communicate with customers, investors, employees, and other stakeholders. As technology continues to advance, the importance of social media cannot be understated. While organizations benefit from social media, they are only starting to become aware of the risk associated with its use in the workplace (DiStaso and McCorkindale, 2013; Larcker et al., 2012; Russell Herder and Ethos Business Law, 2009). The practitioner literature suggests that a majority of organizations may be following a reactive approach to social media risk management, as opposed to the proactive approach indicated by risk management best practices (Larcker et al., 2012; Scott and Jacka, 2011). However, there is little academic research addressing this issue. To close this gap, this paper develops and tests a set of hypotheses based on the assumption that organizations follow a reactive approach to managing their social media risks.

Drawing from the risk management principles of the ERM-IF, we develop a model that incorporates four components: (i) social media use, (ii) the perceived risk of use, (iii) policy implementation, and (iv) training and technical controls. We tested the model by surveying risk management, audit, and finance professionals. Results from 98 participants confirm predictions that social media use increases the perceived risk of use, the perceived risk of use moderates the effect of social media use on policy implementation, and that policy implementation increases the extent of social media-related training and technical controls. In a supplemental analysis, we tested whether the perceived risk of use mediates the relation between social media use and policy implementation and find that the

[1] The Tenenhaus Goodness of Fit (GoF) statistic provides a means of determining the explanatory power of PLS models (Kock, 2015). The thresholds of effect size are similar to the Cohen (1988) thresholds used in structural equation modeling (SEM), i.e., small ≥ 0.10, medium ≥ 0.25, and large ≥ 0.36.

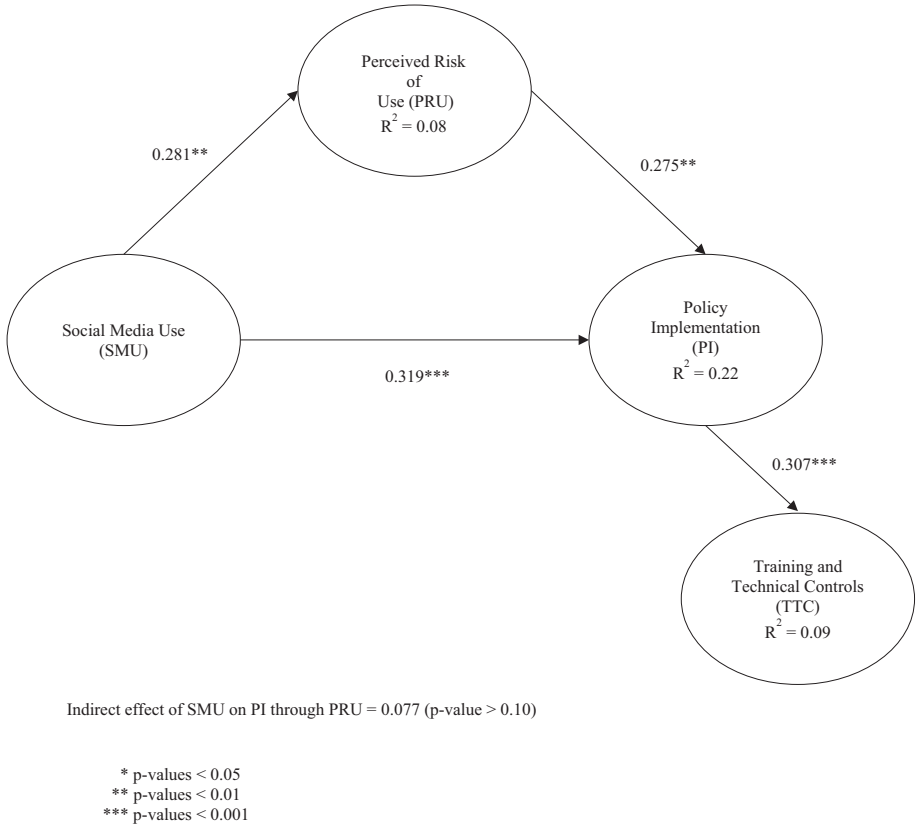

Fig. 3. Supplemental analysis.

indirect relation between social media use and policy implementation is not significant. Overall, the results from our hypotheses testing and supplemental analysis provide evidence that organizations are taking a reactive, rather than a proactive approach to social media risk management. This suggests that organizations are implementing social media policies on an ad hoc basis, without using a formalized risk management process per best practices indicated by the ERM-IF.

In addition, this result supports the notion that many organizations have insufficiently adopted risk management strategies across all their systems (Arena et al., 2010; Hayne and Free, 2014; Power, 2007, 2009). It is also consistent with the idea that organizations are deploying social media without carefully developed risk management processes, due to the fact that this technology is easy to adopt and implement without the structured processes that typically accompany the adoption of other information technologies (Aggarwal and Singh, 2013; Baird and Parasnis, 2011; Heinrichs et al., 2011; Scott and Jacka, 2011). The SM-RMM provides a framework that organizations can use to address this problem, since it describes a risk assessment and risk management methodology that applies specifically to organizational social media use.

There are several limitations to this study. First, risk management best practices indicate there are four responses to managing risk: avoid, accept, share, or reduce the risk (COSO, 2004). Avoidance is an unlikely strategy since, once an organization has begun to use social media, it is difficult to change course and avoid social media use. Even though Brivot et al. (2017) observe that a small number of organizations with well-established reputations make a deliberate decision to avoid social media, the number of such organizations is declining over time. Therefore, it is likely that organizations will use some combination of the other three responses to manage social media risk. While the results indicate that organizations are taking a reactive approach to social media risk management and implementing policies on an ad hoc basis, we are unable to distinguish if these policies reflect an organization's choice to accept, share, or reduce social media risk.

Second, the study analyzes respondents' perceptions of their organizations' social media risk management policies at a given point in time. Thus, it does not examine how social media risk management evolves in response to feedback from within and outside the organization. For example, the monitoring component of the ERM-IF indicates that an organization must monitor the efficacy of its risk management activities and make modifications as necessary (COSO, 2004).

Third, the results are based on a fairly short survey with a limited number of questions. For example, to keep the survey at a manageable length, respondents were asked six questions each about social media use and perceived risk of use. They also were not asked detailed questions about their organizations' training programs or technical controls related to social media risk.

Fourth, our sample size was not large enough to assess whether there were meaningful differences in social media use, perceived risk of use, and policy implementation across different industries and types of organizations (e.g., public, private, government, or not-

for-profit). The sample also was not large enough to assess whether social media risk perceptions varied depending on the respondent's role in an organization.

Finally, the study does not distinguish between social media use on desktop computers versus mobile devices. Social media use on mobile devices is rapidly increasing (Adobe, 2015; Comscore, 2013). Indeed, 77% of social media is accessed via mobile devices (Investis, 2015). Workplace-related social media use on mobile devices might pose an especially high level of IT security and information leakage risk, as mobile devices typically are not subject to the same controls and monitoring as an organization's computers (Crossler et al., 2014; ISACA, 2010).

To address these limitations, we make the following recommendations for future research. While this study suggests that organizations may adopt social media policies without following formalized risk management processes, it does not indicate how or why this occurs. A qualitative small-sample study based on interviews of risk managers, internal auditors, and others involved in social media risk management can provide insights into this important issue. This type of research can also examine whether organizations that follow a formalized risk management process are maximizing the opportunities and minimizing the risks of social media better than organizations that do not follow such processes. This is important, given that the failure to manage social media risks can have a significant detrimental effect on firm profitability (IRM, 2002; Scott and Jacka, 2011).

Future research can also examine more detailed questions about the relationship between different types of social media use and associated perceived risks, especially since research has documented a number of different ways that business managers employ and gain value from social media (Schaupp and Bélanger, 2014). Similarly, future research can examine individual social media risks in further depth. These include public company disclosure compliance risk (SEC, 2013), information privacy and security risk (ISACA, 2010), and the risks associated with workplace-related social media use on mobile devices (Crossler et al., 2014).

Finally, future research can examine how the strategies of accepting, sharing, or reducing social media risk lead to different policies. It might also expand the SM-RMM to include internal monitoring and external intelligence elements. Such research would support the idea that social media risk management is not just a one-time effort, but rather, a continual process of incremental improvement and evolution (Lee and Green, 2015).

Acknowledgements

We thank the 2012 Pacific Northwest Enterprise Risk Forum for their assistance in data collection and acknowledge helpful comments from Rob Pinsker, anonymous reviewers from the 2014 Accounting Information Systems Midyear Meeting and the 2014 Florida Accounting Behavioral Research Symposium and research assistance from Kaia Marcinkowski.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.accinf.2017.12.004.

References

Accenture, 2014. A comprehensive approach to managing social media risk and compliance. https://www.accenture.com/us-en/insight-comprehensive-approach-managing-social-media-risk.aspx.
Adobe, 2015. Mobile Consumer Survey Results. http://landing.adobe.com/en/na/solutions/experience-manager/188465-mobile-consumer-study.html.
Aggarwal, R., Singh, H., 2013. Differential influence of blogs across different stages of decision making: bhe case of venture capitalists. MIS Q. 37 (4), 1093–1112.
Arena, M., Arhaboldi, M., Azzone, G., 2010. The organizational dynamics of Enterprise risk management. Acc. Organ. Soc. 35 (7), 659–675.
Arnaboldi, M., Busco, C., Cuganesan, S., 2017. Accounting, accountability, social media and big data: revolution or hype? Account. Audit. Account. J. 30 (4), 762–776.
Baird, C.H., Parasnis, G., 2011. From social media to social customer relationship management. Strateg. Leadersh. 39 (5), 30–37.
Bennett, W.L., 2008. Changing citizenship in the digital age. In: Bennett, W.L. (Ed.), In Civic Life Online: Learning How Digital Media Can Engage Youth. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning MIT, Cambridge, MA.
Bockius, C., Selby, S.F., 2011. Social media: roadmap to adoption. LIMRA's MarketFacts Quarterly 31 (2), 52–57.
Brivot, M., Gendron, Y., Guenin, H., 2017. Reinventing organizational control: meaning contest surrounding reputational risk controllability in the social media area. Account. Audit. Account. J. 30 (4), 795–820.
Castillo, C., Mendoza, M., Poblete, B., 2011. Information credibility on twitter. In: Proceedings of the 20th International Conference on the World Wide Web. Association for Computing Machinery, pp. 675–684.
Chan, W., Leung, E., Pili, H., 2012. Enterprise risk management for cloud computing. http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf.
Cohen, J., 1988. Statistical Power Analysis for the Behavioral Sciences. Lawrence Erlbaum, Hillsdale, NJ.
Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004. Enterprise Risk Management – Integrated Framework. http://www.coso.org/guidance.htm.
Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2013. Internal Control – Integrated Framework. http://www.coso.org/guidance.htm.
Comscore, 2013. Mobile Future in Focus. http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_Mobile_Future_in_Focus3.
Constantin, L., 2014. 5 things you need to know about cybersecurity insurance. http://www.cio.com/article/2376802/security0/5-things-you-need-to-know-about-cybersecurity-insurance.html.
Crossler, R.E., Long, J.H., Loraas, T.M., Trinkle, B.S., 2014. Understanding compliance with bring your own device policies utilizing protection motivation theory: bridging the intention-behavior gap. J. Inf. Syst. 28 (1), 209–226.
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 Q. Exec. 9 (4), 243–259.
Deans, P.C., 2011. The impact of social media on c-level roles. MIS Q. Exec. 10 (4), 187–200.
Deloitte, 2009. Social Networking and Reputational Risk in the Workplace. http://www.deloitte.com/assets/dcom-unitedstates/local%20assets/documents/us_2009_ethics_workplace_survey_220509.pdf.
Deloitte, 2012. Aftershock: Adjusting to the New World of Risk Management. http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Services/Risk%20services/Deloitte_Aftershock_Adjusting_to_the_new_world_of_risk_management_July_2012.pdf.
DiStaso, M.W., McCorkindale, T., 2013. A benchmark analysis of the strategic use of social media for Fortune's most-admired U.S. companies on Facebook, Twitter, and You Tube. Public Relat. J. 7 (1), 1–33.
ElBoghdady, D., 2013. SEC Clears Up 'Confusion' over Social Media Rules. Washington Post. http://articles.washingtonpost.com/2013-04-02/business/38218852_1_reed-hastings-netflix-spokesman-facebook-page.
Engen, J.R., 2012. The lure of corporate social media. https://www.boardmember.com/Print.aspx?id=7870.

Ernst & Young, 2012. Social Media Strategy, Policy and Governance. http://www.ey.com/Publication/vwLUAssets/Social_media_strategy_policy_and_governance/$File/Social_media_strategy_policy_governance.pdf.
Ernst & Young, 2014a. The Business of Social Media: Strengthening and Protecting Your Brand. http://www.ey.com/US/en/Issues/Governance-and-reporting/Audit-Committee/BoardMatters-Quarterly—April-2014—4—The-business-of-social-media.
Ernst & Young, 2014b. Harnessing the Power of Data: How Internal Audit Can Embed Data Analytics and Drive More Value. http://www.ey.com/Publication/vwLUAssets/EY-internal-audit-harnessing-the-power-of-analytics/$FILE/EY-internal-audit-harnessing-the-power-of-analytics.pdf.
Eschenbrenner, B., Nah, F.F.H., Telaprolu, V.R., 2015. Efficacy of social media utilization by public accounting firms: findings and directions for future research. J. Inf. Syst. 29 (2), 5–21.
Field, J., Chelliah, J., 2012. Social-media misuse a ticking time-bomb for employers: robust policies and procedures needed to reduce the risks. Hum. Resour. Manag. Int. Dig. 20 (7), 36–38.
Fornell, C., Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement. J. Mark. Res. 18 (1), 39–50.
Galligan, M.E., Rau, K.K., 2015. COSO in the cyber age. http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf.
Geyer, S., Krumay, B., 2015. Development of a social media maturity model – a grounded theory approach. Proceedings, 48th Hawaii international conference on system sciences. http://ieeexplore.ieee.org/document/7070035/?arnumber=7070035&tag=1.
Greene, S., O'Brien, C.N., 2013. Exceeding authorized access in the workplace: prosecuting disloyal conduct under the computer fraud and abuse act. Am. Bus. Law J. 50 (2), 281–335.
Greenwald, D., 2010. Social media: changing the world of business communication. In: Proceedings of the 75th Annual Convention of the Association for Business Communication (October 27–30). IL, Chicago.
Haimes, Y.Y., 2012. Systems-based guiding principles for risk modeling, planning, assessment, management, and communication. Risk Anal. 32 (9), 1451–1467.
Hair, J.F., Ringle, C.M., Sarstedt, M., 2011. PLS-SEM: indeed a silver bullet. J. Mark. Theory Pract. 19 (2), 139–150.
Hair, J.F., Sarstedt, M., Ringle, C.M., Mena, J.A., 2012. An assessment of the use of partial least squares structural equation modeling in marketing research. J. Acad. Mark. Sci. 40 (1), 414–433.
Hayne, C., Free, C., 2014. Hybridized professional groups and institutional works: COSO and the rise of enterprise risk management. Acc. Organ. Soc. 39 (6), 309–330.
He, W., 2012. A review of social media security risks and mitigation techniques. J. Syst. Inform. Technol. 14 (2), 171–180.
Heinrichs, J.H., Lim, J.S., Lim, K.S., 2011. Influence of social networking site and user access method on social media evaluation. J. Consum. Behav. 10 (6), 347–355.
Hildebrand, C., Haubl, G., Herrmann, A., Landwehr, J.R., 2013. When social media can be bad for you: community feedback stifles consumer creativity and reduces satisfaction with self-designed products. Inf. Syst. Res. 24 (1), 14–29.
Institute of Risk Management (IRM), 2002. A Risk Management Standard. http://www.theirm.org.
Investis, 2015. Social Media for Corporate Communications: A Review of Corporate Social Media Use in the US and the UK. http://info.investis.com/basic-page/social-media-review.
ISACA, 2010. Social Media: Business Benefits and Security, Governance and Assurance Perspectives. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Social-Media-Business-Benefits-and-Security-Governance-and-Assurance-Perspectives.aspx.
ISACA, 2011. Social Media Audit/Assurance Program. Rolling Meadows, IL.
Kane, G.C., Alavi, M., Labianca, G., Borgatti, S., 2014. What's different about social media networks? A framework and research agenda. MIS Q. 38 (1), 275–304.
Kaplan, A.M., Haenlein, M., 2010. Users of the world, unite! The challenges and opportunities of social media. Bu. Horiz. 53, 59–68.
Katz, D.A., McIntosh, L.A., 2013. The Board, Social Media, and Regulation FD. New York Law Journal. http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202593797448&The_Board_Social_Media_and_Regulation_FD&slreturn=20130903163742.
Khansa, L., Kuem, J., Siponen, M., Kim, S.S., 2017. To cyberloaf or not to cyberloaf: the impact of the announcement of formal organizational controls. J. Manag. Inf. Syst. 34 (1), 141–176.
Kock, N., 2010. Using WarpPLS in e-collaboration studies: an overview of five main analysis steps. Int. J. e-Collab. 6 (4), 1–11.
Kock, N., 2014a. Dichotomous Variables. WarpPLS Blog. http://warppls.blogspot.com/2014/05/dichotomous-variables.html.
Kock, N., 2014b. Advanced mediating effects tests, multi-group analyses, and measurement model assessments in PLS-based SEM. Int. J. e-Collab. 10 (1), 1–13.
Kock, N., 2015. WarpPLS 5.0 User Manual. ScriptWarp Systems, Laredo, Texas.
Kock, N., Lynn, G.S., 2012. Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations. J. Assoc. Inf. Syst. 13 (7), 546–580.
KPMG, 2013. Social media: A double-edged sword, to be handled with care. http://www.kpmginstitutes.com/aci/insights/2013/social-media-governance.aspx.
Langheinrich, M., Karjoth, G., 2010. Social networking and the risk to companies and institutions. Inf. Secur. Tech. Rep. 15, 51–56.
Larcker, D.F., Larcker, S.M., Tayan, B., 2012. Director Notes: What Do Corporate Directors and Senior Managers Know about Social Media? The Conference Board, Inc. http://www.gsb.stanford.edu/sites/default/files/documents/TCB_DN-V4N20-12.Social_Media.pdf.
Lee, L., Green, E., 2015. Systems thinking and its implications in enterprise risk management. J. Inf. Syst. 29 (2), 195–210.
Leonardi, P., 2014. Social media, knowledge sharing, and innovation: toward a theory of communication visibility. Inf. Syst. Res. 25 (4), 796–816.
Michaelidou, N., Siamagka, N.T., Christoduolides, G., 2011. Usage, barriers and measurement of social media marketing: an exploratory investigation of small and medium B2B brands. Ind. Mark. Manag. 40 (7), 1153–1159.
Microsoft, 2013. Bring your Own Service: Employees Want Social Tools at Work. Despite Company Restrictions and Hesitation, Reports New Microsoft Survey. http://www.microsoft.com/en-us/news/press/2013/may13/05-27socialtoolspr.aspx.
O'Leary, D.E., 2011a. Blog mining-review and extensions: from each according to his opinion. Decis. Support. Syst. 51 (4), 821–830.
O'Leary, D.E., 2011b. The use of social media in the supply chain: survey and extensions. Intell. Syst. Account. Financ. Manag. 18, 121–144.
Ollier-Malaterre, A., Rothbard, N.P., Berg, J., 2013. When worlds collide in cyberspace: how boundary work in online social networks impacts professional relationships. Acad. Manag. Rev. 38 (4), 645–669.
Perry, L., 2009. Businesses to Make Greater Use of Social Media in 2010. NewsPR.us and OfficialWire. http://dsl-marketing.blogspot.com/2009/12/businesses-to-make-greater-use-of.html.
Power, M., 2007. Organized Uncertainty: Designing a World of Risk Management. Oxford University Press, Oxford.
Power, M., 2009. The risk management of nothing. Acc. Organ. Soc. 34, 849–855.
Preacher, K.J., Hayes, A.F., 2004. SPSS and SAS procedures for estimating indirect effects in simple mediation models. Behav. Res. Methods 36 (4), 717–731.
Preacher, K.J., Hayes, A.F., 2008. Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behav. Res. Methods 40 (3), 879–891.
Preece, J., Shneiderman, B., 2009. The reader-to-leader framework: motivating technology-mediated social participation. Transactions on. Hum. Comput. Interact. 1 (1), 13–32.
Protiviti, 2015. Internal Audit Capabilities and Needs. http://www.protiviti.com/IAsurvey.
Ravichandran, T., Liu, Y., 2011. Environmental factors, managerial processes, and information technology investment strategies. Decis. Sci. 42 (3), 537–574.
Rose, C., 2011. The security implications of ubiquitous social media. Int. J. Manag. Inf. Syst. 15 (1), 35–40.
Russell Herder, Ethos Business Law, 2009. Social media: embracing the opportunities, averting the risks. http://russellherder.com/white-papers/.
Schaupp, L.C., Bélanger, F., 2014. The value of social media for small businesses. J. Inf. Syst. 28 (1), 187–208.
Scott, P.R., Jacka, J.M., 2011. Auditing Social Media: A Governance and Risk Guide. John Wiley & Sons, Hoboken, NJ.
Securities and Exchange Commission (SEC), 2013. SEC says social media ok for company announcements if investors are alerted. http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171513574#.UkucTyEo5jo.
Smith, M., 2013. Microsoft study shatters myth, says social media use increases work productivity. http://www.networkworld.com/community/print/83156.
Thornton, Grant, 2013. Social Media Risks and Rewards. https://www.grantthornton.com/~/media/content-page-files/advisory/pdfs/2013/ADV-social-media-survey.ashx.
Trinkle, B., Crossler, R., Bélanger, F., 2015. Voluntary disclosures via social media and the role of comments. J. Inf. Syst. 29 (2), 101–122.
Tysiac, K., 2012. Tweet this: Social Media Emerging as a Top Risk. Chartered Global Management Accountant Magazine. http://www.cgma.org/Magazine/News/Pages/20126215.aspx.
van Zyl, A.S., 2009. The impact of social networking 2.0 on organizations. Electron. Libr. 27 (6), 906–918.
Wilkin, C.L., Chenhall, R.H., 2010. A review of IT governance: a taxonomy to inform accounting information systems. J. Inf. Syst. 24 (2), 107–146.