KNOWLEDGE PROTECTION CHALLENGES OF SOCIAL MEDIA ENCOUNTERED BY COMPANIES

Abstract

Although social media (SM) represents an entirely new means of creating and sharing knowledge, it also presents entirely new challenges in protecting confidential information and other data that companies do not want to share. Companies that want to use SM for knowledge creation and sharing have to ensure they are able to provide adequate protection of their knowledge. However, knowledge protection and security-oriented knowledge management processes have received little attention in prior studies. This research attempts to close that gap; it examines which information and knowledge protection challenges arise from SM, and why they arise. Our three main findings include 1) a number of challenges for knowledge protection in social media, 2) a number of special characteristics of social media, which are causes for the knowledge protection challenges, and 3) a number of questions that, when answered by the company, can help to react to the identified knowledge protection challenges. Our findings increase the understanding of the dynamics between information security, knowledge protection, and the special characteristics of social media. In addition, our findings open up a number of future research questions and provide companies a tool for creating knowledge protection policies concerning the use of SM.

Keywords: Case study, Information security, Knowledge management, Knowledge protection, Social media, Qualitative research.

1 Introduction

Although information technology (IT) plays an important role in organizational knowledge management efforts (Alavi and Leidner 2001; Tanriverdi 2005), little attention has been paid to the unintended consequences of managing organizational knowledge in information systems (IS) based knowledge management research (Schultze and Leidner 2002). Knowledge management strategies are concerned with the creation, transfer, and protection of knowledge (Bloodgood and Salisbury 2001). Although recently, the use of social media (SM) in organizations has become more popular (Kuikka and Äkkinen 2011; Light et al. 2008), previous research on SM focused on how companies can use it to improve communication and collaboration both within (Annabi et al. 2012) and across (Katzy et al. 2012) organizational borders. Most prior research focused on opportunities SM represents for knowledge creation and knowledge sharing with co-workers (Andriole 2010; Barzilai-Nahon and Mason 2010; Ford and Staples 2010; Katzy et al. 2012; Seebach 2012) and customers; for example, by using online communities for open innovation activities (Dahan and Hauser 2002; Franke and Shah 2003; Kane et al. 2012; Wasko and Faraj 2005). However, knowledge shared and exchanged via SM differs from traditional media because with SM, the content is posted in a public community, while with the later, communication is private (Cao et al. 2012). In comparison with more traditional knowledge management systems, primarily used inside the company without open interfaces with customers, etc., SM is already widely used by individuals to share information with their friends and peers (Light et al. 2008). Employees have a different attitude toward SM than traditional knowledge sharing systems. This represents a challenge for knowledge management and raises new questions concerning protection of knowledge in SM, especially when using it across organizational boundaries.

Ford and Staples (2010) stress that whether and what knowledge is being protected in an organization cannot be generalized and depends on the specific situation and company. Although knowledge protection has indeed been identified as an important topic in the field of knowledge management (Bloodgood and Salisbury 2001; Earl 2001; Ford and Staples 2010), security-oriented knowledge management processes, which are designed to protect the knowledge within an organization from illegal or inappropriate use or theft, have received little attention in the literature (Gold et al. 2001). While organizations and individuals using SM exchange considerable amounts of information, this information is also a high value asset from a knowledge management perspective, and the need to protect it is a key reason why information security is becoming an increasingly important area of interest (Dhillon and Backhouse 2001; Siponen 2005). Companies that want to use SM for knowledge creation and sharing have to ensure that they are able to safeguard their own knowledge base. Recent worries concerning knowledge protection have been voiced in the SM context (Andriole 2010; Harden 2012). In order for companies to be able to react to knowledge protection challenges, they have to know why and in which ways social media represents a threat to knowledge protection. This area represents a clear research gap, which the present research attempts to close by applying an information security perspective and trying to answer the question *"What are the challenges for information and knowledge protection that arise from employees' use of SM, and why do they arise?"*

The paper is organized as follows. Section 2 reviews the literature on knowledge management, social media, and challenges of social media to information and knowledge protection. Section 3 outlines the research methodology. The fourth section presents the findings of our qualitative data analysis: knowledge protection challenges of social media, special characteristics of social

media which are a cause for knowledge protection challenges, and a number of questions arising from these challenges and special characteristics. Section 5 discusses the theoretical implications of our research findings. The study concludes with a summary of the contributions of this study, the implications for practice, the research limitations, and suggestions for future research.

2 Theory

2.1 Knowledge and knowledge management

Knowledge has been identified as a valuable resource for organizational growth (Wasko and Faraj 2000). Carlile (2002) presents three different views of knowledge: 1) mechanistic views focused on knowledge as something to capture, store, and transfer, 2) the cultural view emphasizes the requirements of social interaction in translating knowledge before it can be shared, and 3) the "contested" or "political" nature of knowledge has been stressed. Wasko and Faraj (2000) point out that knowledge can be seen as an object, as embedded in people, or as embedded in the community. Knowledge can be divided into explicit (objective) and tacit (subjective) knowledge. Tacit knowledge consists of received experiences, is implicit in nature, emerges over time, and is therefore difficult to express and manage. Explicit knowledge consists of rational, deducted knowledge; it is easily expressed, can be written down, and passed verbally to others; therefore, it is typically more easily transferred (Bloodgood and Salisbury 2001; Nonaka and Takeuchi 1995). Nonaka (1994: 15) distinguishes between "information" and "knowledge": information is defined as "a flow of messages or meanings which might add to, restructure, or change knowledge," while knowledge is "created and organized by the very flow of information, anchored on the commitment and beliefs of its holder." According to Stenmark (2002), knowledge is the tacit part of our tradition and experiences, while information is the small part we are able to articulate. He argues that tacit knowledge can be articulated into

information. Since the present research examines which knowledge protection challenges exist in social media environments and why, we will specifically look at how to protect the part of knowledge that can be articulated and shared in SM, namely information. Information protection, in turn, is the basis for knowledge protection. Few previous studies on social media and knowledge management clearly distinguish between information and knowledge; indeed, these terms are often used interchangeably. Consequently, we consider studies on both *information* and *knowledge* management and protection in our review of the previous research.

Knowledge management is a multidimensional concept; definitions and interpretations about it abound (Alavi and Leidner 2001; Lloria 2008; Schultze and Leidner 2002; Wasko and Faraj 2000). There are two paradigms of organizational knowledge management. In the organizational management of knowledge literature, knowledge is conceived as situated within a specific workgroup with distinct sociocultural rules, norms, and shared understandings. In the more technically oriented, knowledge-based systems literature, the use of information and computer technologies to communicate knowledge among distributed workgroups depends on the capture, storage, and transfer of knowledge between individuals in many different locations (Gasson and Shelfer 2007). Knowledge management in the present research is understood as with Schulze and Leidner (2002) who define knowledge management as "the generation, representation, storage, transfer, transformation, application, embedding, and protecting of organizational knowledge." According to Bloodgood and Salisbury (2001), companies can gain competitive advantage with the assistance of three knowledge management strategies: *knowledge creation, knowledge transfer,* and *knowledge protection*.

Carlile (2002) emphasizes that organizations must establish processes for managing knowledge across boundaries. The successful sharing of knowledge across boundaries must be conducted by

group members (Barzilai-Nahon and Mason 2010; Carlile 2002; Ciborra and Andreu 2001). Levina and Vaast (2008) maintain that each circumstance of knowledge sharing presents a different combination of boundaries because of the different internal and external dynamics, which have an effect on collaboration and aims. Individuals are not always interested in sharing all types of knowledge, and the organizational culture has an important effect on whether individuals are willing to exchange knowledge (Wasko and Faraj 2000). Not only might the employees be unwilling to share knowledge, but also the company itself might want to prevent information and knowledge sharing across the organization's boundaries. Organizations using a knowledge protection strategy focus on maintaining knowledge in its original and constructive state; thus, preventing it from being altered, transferred to other organizations, lost, or becoming obsolete (Bloodgood and Salisbury 2001). However, as Gold et al. (2001) emphasize, security-oriented knowledge management processes, which are designed to protect the knowledge within an organization from illegal or inappropriate use or theft, have received little attention in the literature. The present study investigates what challenges SM represents for knowledge protection and how. In the next section, we review previous research on information and knowledge management and protection in the context of SM.

2.2 Social media and challenges for knowledge management

Kaplan and Haenlein (2010: 61) define social media 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.*" Previous research studied the roles of, and challenges posed by, SM to individuals and organizations from a number of perspectives. Given that information sharing is not only a technical challenge but also a security and trust problem (Andriole 2010; Barzilai-Nahon and Mason 2010; Bulgurcu et al. 2010; Ford and Staples 2010;

Harden 2012), understanding how SM facilitates the exchange of knowledge in an organizational context is extremely important (Kuikka and Äkkinen 2011; Light et al. 2008; Seebach 2012). Katzy et al. (2012) argue that because SM platforms extend across the boundaries of a firm, SM is bringing significant change to knowledge production. They stress that the younger generation expresses different values toward the work they do, and their behavioral norms appear more relaxed. Consequently, the younger generation appears to treat knowledge as a commodity easily accessed from sources outside the firm boundaries. Barzilai-Nahon and Mason (2010) maintain that members of this generation might have developed skills, habits, and behavioral norms of using technology that differ from those of previous generations. Indeed, often without even considering its flow beyond organizational boundaries, earlier knowledge management studies focused primarily on internal stock and the flow of knowledge as assets closed within organizations. By enhancing knowledge flows in organizations, SM provides individuals with formal and informal ties to knowledge sources both within *and beyond* organizational boundaries. As a result, management and organizational practices become more dynamic and complex (Kim and Benbasat 2012). In the context of our research question, paying special attention to challenges related to the protection of knowledge, next we will summarize the challenges that previous research identified as relevant from an organizational knowledge management perspective in relation to SM.

Without security-oriented processes, knowledge loses the qualities of being rare and inimitable, which are requisite for it to be a source of competitive advantage (Gold et al. 2001); users might additionally underestimate the dangers of publicly posted materials on the web (Donath 2007; Jagatic et al. 2007; Light et al. 2008). Specifically, in the context of knowledge sharing, **challenges related to information security** of SM have been discussed (Harden 2012; Katzy et

al. 2012). Blakley et al. (2001: 97) argue that "information security is required because the application of technology to information creates risks" and that ***confidential information might be disclosed*** (see also Skeels and Grudin 2009), modified in an inappropriate way, destroyed, or lost, which can result in financial loss, damage to reputation, etc. Gross and Acquisti (2005) argue that a lack of privacy in SM networks increases the risk of ***identity theft***. Light et al. (2008) maintain that users trust in the privacy of social network sites; assuming these sites are "closed worlds," they publish provocative material. Malik and Malik (2011) see privacy in growing social networks as a challenge as well. They argue that disclosing personal information in social networks is a double-edged sword: on the one hand, disclosure is a plus or even a must if people want to participate in social networks. On the other hand, disclosing personal information can invite malicious attacks like ***phishing, spamming, and distribution of malware, making identity theft easier, and scams easier***.

Many companies use social networking technology in their marketing efforts—to communicate with customers and attract new business (Light et al. 2008). However, as Aula (2010) argues, SM can also represent a **reputation risk** when using it for corporate communication. Regarding reputation management, he holds that it is imperative to remember that SM content cannot be controlled in advance, and that content cannot be managed in the same way as TV and newspapers (Aula 2010). Kaplan and Haenlein (2010) advise companies to remember that the integration of SM and traditional media is key, as these two arenas are both part of the company's corporate image, and thus of the company's reputation. Kuikka and Äkkinen (2011) also point out that the use of SM in a company can represent reputation challenges.

As discussed above, organizations should establish **processes for managing knowledge** across boundaries (Carlile 2002). Skeels and Grudin (2009) studied the tensions that can arise when

social networks cross hierarchy, status or power boundaries at the workplace (for example, when people feel "forced" to connect with their boss, customers, or co-workers). They discuss the reality that questions concerning the ***legitimacy of using SM at the workplace*** can represent challenges for companies who do intend to use SM. Light et al. (2008) point out that Facebook accelerates the ***merging of people's home and work life***, simultaneously making these different roles both more public and more difficult to manage. Kuikka and Äkkinen (2011) identified identity challenges, the question of distinction between a person's professional and private identity, as a challenge for companies who intend to use SM. In addition, they also identify *ownership challenges* (who is responsible for SM in the company), *authorization challenges* (who is allowed to contribute to SM), and *attitude challenges* (employees' attitude toward the use of SM), which are also relevant from a knowledge management perspective.

Based on previous research, SM represents challenges for a company's knowledge protection in relation to information security (identity theft, scams, and phishing; disclosure of confidential information), to the company's reputation, and to management of SM (crossing boundaries with SM; legitimacy of using SM at the workplace; merging of private and professional identity; questions regarding ownership, authorization and attitude). As Blindref (2012) argue, SM does not appear to represent a significantly greater information security threat from outside attacks (like malware and spam) than other forms of media, and these threats can be mitigated with technical methods. Therefore, the present research will not focus on technological information security challenges but on challenges arising from employee behavior in social media.

3 Methodology

The present research utilized a case study approach. **Case study research** is useful in examining "why" and "how" questions since they have an explanatory character and "deal with operational

links needing to be traced over time, rather than mere frequencies or incidents" (Benbasat et al. 1987). The present research is concerned with studying what challenges for information and knowledge protection arise from SM, and why. Case study research is particularly useful "where research and theory are at their early, formative stages" (Benbasat et al. 1987). The challenges that SM represents for organizational knowledge protection efforts are yet unexplored; therefore, the case study offers a suitable research method for the present study, which involved a qualitative, explanatory case study (Yin 2003).

Regarding the **research setting**: this study is part of a broader research initiative, wherein the present research concentrated on the greatest challenges that SM represents to information security and knowledge protection. Before completing the research, we conducted preliminary interviews with eight specialists in the SM and information security fields to identify topics in need of further analysis. For the actual research, since they are in a suitable position to evaluate the challenges SM represents for information and knowledge protection, we specifically selected informants with extensive experience with information security. The interviewees and the companies all wanted to remain anonymous. To obtain a broader understanding of the issue under study, we conducted interviews in one European country, in organizations of different sizes (from SME to large multinational organizations), and in both the public and private sector. We presented part of our findings from a strict information security perspective in Blindref (2012), whereas the present study focuses on the implications from a knowledge management and protection perspective.

During the **data collection**, we conducted eleven semi-structured interviews (see Myers and Newman 2007) in January and February 2011. Interviews lasted from 30 to 59 minutes (average 47 minutes), which equals a total of 88 pages of transcribed text. For the **data analysis**, we

implemented the following of Eisenhardt's (1989) steps of building theory from case study research: overlap of data analysis with data collection, analyzing within-case data, searching for cross-case patterns, shaping hypothesis, and enfolding literature. We used the NVivo software tool to help conduct the data analysis. We used the challenges identified in relation to information and knowledge protection in Section 2.2 as pre-nodes (identity theft, scams, phishing; disclosure of confidential information; reputation risk; crossing boundaries with SM; legitimacy of using SM at the workplace; merging of private and professional identity; ownership, authorization and attitude toward SM). We subsequently analyzed whether and how they represented challenges for information and knowledge protection in SM specifically for companies. In the analysis, we managed to identify a number of characteristics of SM as a new form of media (information distribution speed; blurry audience; easily collectible information; generation transition), which help to explain why SM represents information and knowledge protection challenges for companies. In addition, we identified a number of questions companies should answer to protect their knowledge in the SM age.

4 Results

In the empirical data analysis, we were able to identify several knowledge protection challenges, as well as a number of special characteristics of SM as a new form of media that proved to be possible causes for one or more knowledge protection challenges, helping to answer the question why social media represents challenges to knowledge protection (see Table 1). Newly identified knowledge protection challenges, and the special characteristics of SM related to these challenges, are marked in italics.

[TABLE 1 HERE]

To demonstrate the relationship between these challenges, we present them in figures with direct citations from the interviewees. In the text, we will add information about which interview the presented information is taken from by adding "Int" and a number from 1 to 11, and adding an additional numeral to make the identification of the correct citation in the figures possible (e.g., Int 5–1 for citation 1 from Interview 5). In Section 4, knowledge protection challenges are identified in bold letters and the related special characteristics of SM as a new form of media in bold and italic letters.

4.1 Information security challenges in knowledge protection

Information security challenges pertain to **identity theft, scams**, and **phishing**. Risks related to scams and phishing are noticeably greater in organizations that clearly have confidential data to protect (Int 1–1). In phishing and identity theft (information is tricked out of, and/or collected about the victim), SM is seen as offering ***easily collectible information*** about others, since anyone can open a SM account under a fake name and impersonate someone else. Another user might allow this "fake" person access to their data without realizing that this other person is indeed a defrauder (Int 10–1, Int 11–1).

Disclosure of confidential information is seen as a risk from a number of different perspectives. Employees can accidently disclose information in SM. This can occur, for example, when writing a blog or posting messages in SM (Int 2–1). One interviewee pointed out that some people do not understand there is a difference between them and the company (Int 5–1). Another interviewee gave an example where an employee posted information on the progress of an international secret operation in a blog, telling what events were going to happen next. As a result, for the next operation, the company provided guidelines for the use of SM (Int 1–2). Employees can also intentionally disclose information. For example, some employees disclosed

knowledge of work conditions because they were not satisfied with their employer (Int 5–2). One challenge related to disclosure of confidential information, and information sharing in general, seems to be the ***blurry audience*** in SM. This was regarded as one reason people are more likely to disclose confidential information in SM—they are not completely aware of with whom they are sharing information. Several information security managers expressed this concern (Int 8–1). However, some interviewees did not see SM as any greater risk to information disclosure than other media (Int 6–1). Another challenge related to disclosure of confidential information appears to be that there are currently different "generations" at work: the younger generation who grew up with SM, and the older generation who start to use SM after having worked in an organization for many years already. As one interviewee expressed, the ***generation transition*** might help to decrease problems related to disclosure of information (Int 2–2). These information security challenges and the citations supporting our findings are presented in Figure 1.

[FIGURE 1 HERE]

4.2 Reputation challenge in knowledge protection

One big concern related to SM is the **reputation challenge** and the control of reputation. How to maintain one's reputation is regarded as the most central risk (Int 3–1). Employees posting "inappropriate" private opinions and pictures in SM are regarded as a potential threat to the organization's reputation. Some companies deny access to social network sites, among other reasons, to prevent bad publicity (Int 7–1). Especially challenging in relation to reputation is the ***information distribution speed*** in SM (Int 3–2, Int 5–3).

Several interviewees considered it a threat that private statements by employees could be interpreted as company statements. Especially with younger employees, the danger of confusing private and professional personas might be higher (Int 7–2), since they grew up with SM and are

accustomed to sharing their opinion in SM. This ***merging of professional and private identity*** in SM is seen by some interviewees as a bigger problem for people on a higher hierarchy level than for those on a lower level, since individuals in higher positions or those who are well-known have a stronger connection to the company in people's minds (Int 5–4). Several interviewees mentioned that they adapt their communications in SM to their work role (Int 6–2, Int 1–3). The merging of professional and private identity is also related to the ***generation transition***, and one interviewee hoped that in 10 years people would understand that individuals could post things in SM without that being connected to their work or employer (H8–2). Figure 2 presents the reputation challenges and the citations supporting our findings.

[FIGURE 2 HERE]

4.3 Management challenges in knowledge protection

Several challenges relate both to the management of SM use in the company and to the role that SM plays in the company. From a knowledge protection perspective, these management challenges bring up a number of questions for the company. One management challenge concerning knowledge protection is the **crossing of boundaries with SM**, including **communication with customers and professional peers**, as well as the collection of information about the company in SM. Some companies use SM to *communicate and connect with customers* through blogs and/or special interest groups. For example, one company uses Facebook as a communication channel (Int 3–3), while another company established a discussion forum where certain employees observe and, if necessary, participate in customer discussions (Int 4–1). However, crossing boundaries in SM can also lead to conflicting situations and it is not always clear, for example, whether and how employees are allowed to connect with customers (Int 2–3). Some companies provide guidelines as to what employees can say about customers

and co-workers in SM (Int 3–4). Employees use SM to *keep in contact and communicate with their colleagues and peers*. LinkedIn received frequent mention as a tool for maintaining a network of professional peers (Int 2–4). Whether an employee uses SM in general also seems to be a ***generation transition*** question (Int 9–1). While some companies actively use SM to **collect information about the company**, i.e., as a source of knowledge concerning what others say about their company in SM (Int 3–5), others just do it ad-hoc, for instance, if someone, by chance, notices something mentioned about the company in SM (Int 7–3). In some organizations, it is not an organizational decision to follow SM, but done through the initiative of individual employees (Int 5–5). It also appears that SM can represent a source of knowledge about the company precisely because of ***easily collectible information*** that is available in SM.

The second management challenge related to knowledge protection in SM concerns the **legitimacy of using SM at the workplace**. Whether the use of SM is allowed in companies seems strongly related to whether the company sees SM as a suitable tool for crossing boundaries. In addition, whether access to SM is allowed also depends on the work role of the employee. SM use is supported in companies that regard it as a channel for connecting with customers (Int 6–3). Another company denied everyone access to certain websites because of malware distribution, and prevented access to all websites but a few from certain computers because the work role of the employees at those computers did not demand internet access (Int 7–4). In one company where SM did not play a large role in the company's business operations, the interviewee thought that the use of SM during work time should be denied altogether (Int 5–6). Figure 3 presents these management challenges and the citations supporting our findings.

[FIGURE 3 HERE]

4.4 Knowledge protection – an integrated framework

In this section, we present the main outcome of our research—a framework describing a number of knowledge protection challenges in SM, and the characteristics of SM as a new form of media, which turned out to be possible causes for one or more knowledge protection challenges. We presented these SM characteristics and knowledge protection challenges in Sections 4.1–4.3. Based on the knowledge protection challenges, which we identified in the empirical data, a number of questions concerning knowledge management arise. Answering these questions can help knowledge management policy makers respond to, or ideally even prevent, the identified knowledge protection challenges. While Table 2 summarizes these questions, it does not give a complete account of knowledge protection challenges that these questions arise from, but instead presents a number of selected examples.

[TABLE 2 HERE]

Figure 4 shows the main contribution of our research: a framework, which integrates our findings on knowledge protection challenges, characteristics of SM as a new form of media, which are possible causes for these challenges, as well as the questions arising from these challenges. We will discuss the most important implications of this framework for knowledge protection in the light of previous research in Section 5.

[FIGURE 4 HERE]

5 Discussion

We will discuss the main contribution of our study, the "Framework of knowledge protection challenges arising from SM as a new form of media," and the questions and challenges for knowledge protection arising when knowledge and information are being actively shared in SM.

5.1 Knowledge protection challenges and questions arising from these challenges

5.1.1 Information security challenges

Information security challenges included risks of identity theft, scams, and phishing in SM, as well as the disclosure of confidential information. Because SM makes it relatively easy to present oneself under a different identity, **identity theft, scams, and phishing** were all seen as challenges in SM. Moreover, the fact that the ***audience in SM is often blurry*** (people are not always aware of how many people see the information they post) makes it more difficult to know with whom one is actually sharing information. Therefore, the question arises as to *whether employees actually share information with whom they think they are sharing*. As Light et al. (2008) point out, users are often not aware that social network sites are not "closed worlds." This lack of awareness contributes to the blurry audience in social media.

The problem of **disclosure of confidential information** is extremely interesting from a knowledge management perspective. Stenmark (2002) argues that information requires knowledge both to be created and to be understood. From a knowledge protection perspective, this means that information shared in SM is not equally valuable to everyone, since it depends on the already existing knowledge-base, which the audience of that information possesses. This represents a tremendous challenge for knowledge protection—how can a company define *what kind of information can be shared in SM* by their employees? When, for example, an employee shares pictures containing a geotag on Facebook while they are on a ship searching for pirates (see Int 1–2, Figure 1), this information will not automatically result in knowledge about the current location of that ship. Someone who does not know, for instance, that such a pirate-hunting operation is currently taking place probably would not be able to create knowledge regarding the position of the pirate-hunting ship based on the shared geotag information. Since it

is almost impossible to know the different knowledge backgrounds of a given audience, and in turn to know what kind of knowledge that audience can create based on the shared information, the blurry audience makes the question *what information can be shared* even more complicated.

5.1.2 Reputation challenges

The **reputation challenge** is strongly related to the challenge of preventing the disclosure of confidential information and to the question of *what kind of information can be shared in SM*. In studying information security from an information risk management perspective, Blakley et al. (2001) point out that improper disclosure of information can have negative effects on the reputation of the company. Companies are worried about employees distributing unfavorable information about the company (for example, see Int 5–2, Figure 1), which in turn could lead to a negative public image of the company. This risk, which was based on our study, is regarded as higher in SM than traditional media. Aula et al. (2010) also maintain that content in SM cannot be controlled in advance and it cannot be managed in the same way as newspapers and television. We add to Aula et al.'s (2010) findings by demonstrating that the ***high information distribution speed*** in SM contributes to this problem. Nevertheless, from a general knowledge management perspective, it is important to acknowledge that the high information distribution speed, which represents a challenge for knowledge protection, is a simultaneous strength of SM when the intent of a company is to share knowledge. In fact, from a general knowledge management perspective, the company has to ponder the advantages and disadvantages of protecting knowledge vs. sharing knowledge (e.g. Kim et al. 2008). A company that is especially protective of their knowledge and takes precautions to prevent inadvertent sharing of knowledge might additionally experience decreased possibilities of creating knowledge and learning by sharing knowledge. As Wenger (2004) explains, in a knowledge economy, reputation is a crucial

asset and sharing knowledge is, therefore, a source of power, providing that one's social community serve as a platform to build a reputation. Hence, SM can indeed help the company to build a reputation, but at the same time, knowledge protection has to ensure that reputation does not suffer from the disclosure of confidential information. Ford and Staples (2010) emphasize that misunderstanding or the misuse of knowledge by a recipient could variously result in organizational harm, loss of profits, or harm the informer's reputation if noted as the original source of the knowledge. Based on our findings, SM makes it more complicated to differentiate between harm to the reputation of the company and harm to the reputation of the individual. Kaplan and Haenlein (2010) advise companies to integrate SM and traditional media, since both are part of the corporate image. This raises the question as to *what role SM plays in the company*.

5.1.3 Management challenges

As discussed in previous research, SM is used to cross boundaries to communicate with customers. In this context, we want to emphasize the difficulty answering the question of *who in the company is allowed to share information in SM*. Kuikka and Äkkinen (2011) regard this as the "authorization challenge" in relation to the adoption and use of SM in organizations. Defining that employee X is allowed to communicate in SM (e.g., with customers), but employee Y is not, is possible in cases where the company actively uses a certain SM forum to interact with its customers. However, in comparison to more traditional media (where it is somewhat easier to define who is allowed to make statements on behalf of the company), practically anyone in the company can share and disclose information about the company and interact with customers in SM. The private use of SM is very common. Furthermore, since it is nearly impossible for the company to observe what employees post during their private use of SM;

based on our findings, this is one of the major challenges for knowledge protection in SM. We will discuss the merging of professional and private identity in more detail in Section 5.2.

Although the initial impression regarding the **collection of information about the company in SM** is that it is not a knowledge protection challenge, it is strongly correlated when analyzing the case of SM in detail. Specifically, the ***easily collectible information*** in SM makes it possible for companies to use SM as a source of information. As Klamma et al. (2007) demonstrate, software tools provide a means to collect information automatically from blogs and other SM sites. Furthermore, the company might not want employee comments on company matters in SM, which goes back to the question o*f who is actually allowed to share information in SM*, and raises the question of *with whom is one allowed to share information in SM*. Since with SM, the content is posted in a public community, Cao et al. (2012) argue that knowledge shared and exchanged via SM differs from that of traditional media. This makes information easily collectible. From the perspective of a company that wants to collect information, this is an opportunity, but for a company that wants to protect knowledge, this characteristic of SM represents a challenge (see Section 5.1.1).

Whether a company pursues a specific goal using SM (customer service, advertising, information collection, etc.) also influences the **legitimacy of using SM at the workplace**. The question of *when employees are allowed to share information in SM*—during work-time, or only during their own free-time—is related to the management challenge of the legitimacy of SM use at the workplace. This question is also strongly correlated to the generation transition (Section 5.2)..

Since they are intertwined with and affect each other, knowledge protection challenges and challenges arising from the characteristics of SM as a new form of media are not straightforward matters. Therefore, to even consider knowledge protection issues related to SM, the company

first has to answer the questions *what role does SM play in the company*, and *who is responsible for SM in the company*. Wasko and Faraj (2000) present three perspectives on knowledge-strategies: 1) knowledge as object, 2) knowledge embedded in people, and 3) knowledge embedded in the community. How a company sees knowledge will probably influence its attitude toward employee use of SM for sharing information. A company that sees knowledge as an object, where ownership of knowledge lies with the company, might see SM as a real threat, since people can easily distribute valuable company knowledge. Companies that see knowledge as embedded in people might see it as useful for improving communication between experts. For companies that see knowledge embedded in the community, SM probably represents a welcome tool for creating and sharing knowledge. Therefore, whether and how a company allows the use of SM from a knowledge protection perspective will also depend on how the company perceives knowledge. Similarly, each employee's view of knowledge has an influence on how that employee behaves in SM. Therefore, when considering how to respond to knowledge protection challenges in SM, the company also should consider the possibility that each employee might understand knowledge differently. Future research on knowledge protection could focus in more detail on the effects different views of knowledge have on knowledge protection challenges. Kuikka and Äkkinen (2011) identify the "ownership challenge" and advise companies who want to use SM to define who is responsible for SM. Our findings indicate this is a relevant question in the context of knowledge protection in SM. In Section 5.1, although we only discussed a few examples of how different questions related to knowledge protection challenges arise, these questions relate to a number of knowledge protection challenges. Furthermore, it also appears that these questions are relevant for knowledge sharing policies, and should be considered in overall knowledge management initiatives.

5.2 Special characteristics of SM create knowledge protection challenges

Our study identified several characteristics of SM, which are possible causes of knowledge protection challenges. These include information distribution speed, blurry audience, merging of professional and private identity, easily collectible information, and generation transition. The previous section briefly discussed blurry audience, information distribution speed, and easily collectible information. In this section, we focus on the identity challenge and generation transition characteristics, which are closely related.

During empirical data analysis, we realized that SM in organizations must be examined from two very different perspectives: 1) SM can be a tool to share knowledge about the organization and to create knowledge, and 2) it is also used privately by employees. The latter perspective is interesting from a knowledge protection perspective, especially in the light of generation transition and the merging of professional and private identity. As Levy (2009) points out, the younger generation already uses Web 2.0 tools (i.e., SM), and therefore expects SM to be available at the workplace. Indeed, they find it natural to use SM. This ***generation transition*** represents an immense challenge for knowledge protection and knowledge management in general. The younger generation's attitude toward sharing information in SM often differs from that of the older generation (Barzilai-Nahon and Mason 2010). Kuikka and Äkkinen (2011) identified the attitude challenge (challenges arising from employees' different attitudes toward the legitimacy of using SM at work) in the situation where a company wants to use SM. We expand these findings by demonstrating that different attitudes toward SM and what can and what cannot be shared in SM, are also related to the generation transition. Conversely, for older employees, it might be easier to understand that certain organization-related knowledge should not be shared in SM. Vodanovich et al. (2010) point out that the younger generation, so-called digital natives, are less cautious with personal information and therefore more vulnerable to

threats and risks that the internet and related technologies pose. Digital natives might not fully appreciate how their information could be misused, and therefore might take risks that the older generation would avoid. Our study indicated that this is also a danger in SM (see Int 7–2, Figure 2). On the other hand, young people might be better aware of the blurry audience in SM, and the speed with which information can spread in SM, since they have grown up with this type of media (Barzilai-Nahon and Mason 2010). This means that organizations also have to consider that different knowledge protection challenges might arise from the older employee generation than from the younger generation.

The concept of "digital natives," developed and discussed by Vodanovich et al. (2010), offers an interesting perspective of the ***merging of professional and private identity***. Vodanovich et al. (2010) argue that previous research on information systems focused on so-called digital immigrants who use information systems mainly in the office for professional reasons. However, there is a lack of studies on the new generation of employees entering the workplace, the digital natives who use ubiquitous information systems for both professional and personal purposes at both the office and at home. Our findings build on those of Vodanovich et al. (2010) by demonstrating that this represents special challenges in the context of SM, where the merging of professional and private identity is prevailing since SM is also widely used by employees for private communication and knowledge sharing outside the office and at home. Furthermore, our study shows that the employee's role in the company has a significant impact on whether a statement published in SM is interpreted as a statement of the company or of a higher person—the higher the position in the company, the more difficult it is to keep statements made under personal and private identity apart (see also Blindref 2012). Our findings further expand on those of Vodanovich et al. (2010) by showing that the merging of professional and private identity is

not only dependent on the generation to which an employee belongs, but also on the role that person has in a company. Therefore, if SM is used within companies to improve knowledge creation and sharing, we believe that the company has to be especially thorough in making certain that employees indeed understand that in the employees' private use of SM, no information and opinions about the company should be shared.

6 Conclusions

This paper examined data collected in a qualitative case study in eleven companies to determine which challenges arise in social media for a company's information and knowledge protection efforts, and why they arise. The main contribution of this study is a framework of knowledge protection challenges arising from social media, which increases understanding of the connection between different challenges, and raises the questions companies should answer when attempting to protect knowledge in the age of social media. We want to emphasize three findings. *First,* certain challenges identified in connection to social media represent specific challenges for knowledge protection. These include information security, reputation, and management challenges. *Second,* we identified a number of special characteristics of social media as a new form of media: information distribution speed, blurry audience, merging of professional and private identity, easily collectible information, and generation transition. These characteristics help explain why knowledge protection challenges arise specifically in connection to SM. *Third,* a number of questions that arise in relation to knowledge protection in social media were identified. These questions represent possible direction for future research, and can help companies respond to the different knowledge protection challenges.

The study also has **practical implications**. In addition to dealing with the challenges arising from employees' private social media use, our framework can assist companies in evaluating the

challenges for knowledge protection if they want to use social media to communicate with customers. Our findings provide companies a tool to create better knowledge protection policies concerning SM use. We believe that answering the questions that arose in relation to the knowledge protection challenges can help organizations achieve greater success in their knowledge protection efforts, and to evaluate possible use of SM in the company for knowledge creation and sharing across organizational boundaries.

Our study has several **limitations**. We did not study knowledge protection challenges of companies using SM in open innovation activities, or who use SM only within their own organizational boundaries for knowledge sharing and creation. Therefore, the results of our study do not automatically apply in those cases and they would need separate testing. We attempted to obtain more generalized insight by studying companies from a number of different industries (both public and private sector). However, the study was conducted in only one European country, which represents a limitation. In this research, we focused specifically on knowledge protection from an organizational perspective, but not on the effects of lacking knowledge protection for an individual person. Furthermore, we focused on the behavioral aspects rather than the technological means of knowledge protection. This also represents a research limitation.

Future research could further examine the effect the type of organization and the role SM plays in the organization have on knowledge protection challenges. A company that actively uses SM and encourages their employees to participate in SM might experience different knowledge protection challenges than a company denying the use of SM. We found indications that both our framework and our findings are relevant from the perspective of knowledge sharing. For example, challenges from a knowledge protection perspective—information distribution speed and easily collectable information—represent opportunities from a knowledge sharing

perspective. Conversely, generation transition, merging of professional and private identity, and blurry audience, equally represent challenges for knowledge creation and knowledge sharing efforts. Future research could also examine, in more detail, the dilemma for companies who have to evaluate the possibilities SM represents to knowledge sharing on the one hand, and the challenges SM represents for knowledge protection on the other. As our findings also appear to be relevant from a knowledge creation and sharing perspective, future research could take these findings and evaluate their implications for general knowledge management.

7 References

Alavi, M. and D. Leidner. "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues." *MIS Quarterly,* 25:1 (2001): 107–136.

Andriole, S. "Business Impact of Web 2.0 Technologies." *Communications of the ACM,* 53:12 (2010): 67–79.

Annabi, H., McGann, S., Pels, S., Arnold P., and C. Rivinus. "Guidelines to Align Communities of Practice with Business Objectives: An Application of Social Media." Proceedings of the 45th Annual Hawaii International Conference on System Sciences, January 2012.

Aula, P. "Social Media, Reputation Risk and Ambient Publicity Management." *Strategy & Leadership,* 38:6 (2010): 43–49.

Barzilai-Nahon, K., and R. M. Mason. "How Executives Perceive the Net Generation." *Information, Communication & Society,* 13:3 (2010): 396–418.

Benbasat, I., Goldstein, D. K., and M. Mead. "The Case Research Strategy in Studies of Information Systems." *MIS Quarterly,* 11:3 (1987): 369–386.

Blakley, B., McDermott, E., and D. Geer. “Information Security is Information Risk Management.” In Proceedings of the NSPW´01, Cloudcroft, New Mexico, USA, 97–104, September 10–13, 2001.

Blindref (2012) – blinded to prevent author identification.

Bloodgood, J. M., and D. Salisbury. “Understanding the Influence of Organizational Change Strategies on Information Technology and Knowledge Management Strategies.” *Decision Support Systems,* 31:1 (2001): 55–69.

Bulgurcu, B., Cavusoglu, H., and I. Benbasat. “Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness.” *MIS Quarterly,* 34:3 (2010): 523–548.

Cao, X., Vogel, D., Guo, X., Liu, H., and J. Gu. “Understanding the Influence of Social Media in the Workplace. An Integration of Media Synchronicity and Social Capital Theories.” Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2012.

Carlile, P. “A Pragmatic View of Knowledge and Boundaries: Boundary Objects in New Product Development.” *Organisation Science,* 13:4 (2002): 442–455.

Ciborra, C., and R. Andreu. “Sharing Knowledge across Boundaries.” *Journal of Information Technology,* 16:2 (2001): 73–81.

Dahan, E., and J. R. Hauser. “The Virtual Customer.” *Journal of Product Innovation Management,* 19 (2002): 332–353.

Dhillon, G., and J. Backhouse. “Current Directions in IS Security Research: Towards Socio-organizational Perspectives.” *Information Systems Journal,* 11:2 (2001): 127–153.

Donath, J. “Signals in Social Supernets.” *Journal of Computer-Mediated Communication,* 13:1 (2007): 231–251.

Earl, M. “Knowledge Management Strategies: Toward a Taxonomy.” *Journal of Management Information Systems,* 18:1 (2001): 215–233.

Eisenhardt, K. M. “Building Theories from Case Study Research.” *The Academy of Management Review,* 14:4 (1989): 532–550.

Ford, D. P., and S. Staples. “Are Full and Partial Knowledge Sharing the Same?” *Knowledge Management,* 14:3 (2010): 394–409.

Franke, N., and S. Shah. “How Communities Support Innovative Activities: An Exploration of Assistance and Sharing Among End-users.” *Research Policy*, 32 (2003): 157–178.

Gasson, S., and K. M. Shelfer. “IT-based Knowledge Management to Support Organisational Learning. Visa Application Screening at the INS.” *Information Technology & People,* 20:4 (2007): 376–399.

Gold, A., Malhotra, A. and A. Segars. “Knowledge Management: An Organizational Capabilities Perspective.” *Journal of Management Information Systems,* 18:1 (2001): 185–214.

Gross, R., and A. Acquisti. “Information Revelation and Privacy in Online Social Networks.” In Proceedings of WPES’05, Alexandria, Virginia, USA, (November 7, 2005): 71–80.

Harden, G. “Knowledge Sharing in the Workplace: A Social Networking Site Assessment.” Proceedings of the 45th Annual Hawaii International Conference on System Sciences, 2012.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and F. Mencze. “Social Phishing,” *Communications of the ACM,* 50:10 (2007): 94–100.

Kane, J., Azad, B., Faraj, S., and A. Majchrzak. “Fostering Innovation and Intellectual Capital Creation: The Paradoxical Influence of Social Media.” *Affordances Journal of Organizational Computing and Electronic Commerce, (JOCEC) (in press).*

Kaplan, A. M., and M. Haenlein. “Users of the World, Unite! The Challenges and Opportunities of Social Media.” *Business Horizons,* 53:1 (2010): 59–68.

Katzy, B., Bondar, K., and R. Mason. “Knowledge-Based Theory of the Firm, Challenges by Social Media.” Proceedings of the 45th Annual Hawaii International Conference on System Sciences, 2012.

Kim, T. H., and I. Benbasat. “Effectiveness of Knowledge Seeking Behaviors Embedded in Social Networks: A Perspective of Individual Workers in Workplaces.” Proceedings of the 45th Annual Hawaii International Conference on System Sciences, 2012.

Kim, Y., Jarvenpaa, S. and A. Majchrzak, “Ad Hoc Interorganizational Collaboration. Safeguards for Balancing Sharing and Protection of Knowledge.” In Becerra-Fernandez, I. and D. Leidner (eds.). *Knowledge Management. An Evolutionary View*. ME Sharp, Armonk, NY, 3008: 292-307.

Klamma, R., Cao, Y., and M. Spaniol. “Watching the Blogosphere: Knowledge Sharing in the Web 2.0.” International Conference on Weblogs and Social Media (*ICWSM),* Boulder, Colorado, USA, 2007.

Kuikka, M., and M. Äkkinen. “Determining the Challenges in Organizational Social Media Adoption and Use.” In Proceedings of the 19th European Conference on Information Systems (ECIS’11), Helsinki, Finland, 2011.

Levina, N., and E. Vaast. “Innovating or Doing as Told? Status Differences and Overlapping Boundaries in Offshore Collaboration.” *Mis Quarterly,* 32:2: (2008): 307–332.

Levy, M. “Web 2.0 Implications on Knowledge Management.” *Journal of Knowledge Management,* 13:1 (2009): 120–134.

Light, B., McGrath, K., and M. Griffiths. “More Than Just Friends? Facebook, Disclosive Ethics and the Morality of Technology.” In the Proceedings of International Conference on Information Systems (ICIS), Paper 193, 2008.

Lloria, M. B. “A Review of the Main Approaches to Knowledge Management.” *Knowledge Management Research & Practice*, 6:1 (2008): 77–89.

Malik, H., and A. S. Malik. “Towards Identifying the Challenges Associated with Emerging Large Scale Social Networks.” *Procedia Computer Science*, 5 (2011): 458–465.

Myers, M. D., and M. Newman. “The Qualitative Interview in IS Research: Examining the Craft.” *Information and Organisation*, 17:1 (2007): 2–26.

Nonaka, I., and H. Takeuchi. *The Knowledge-creating Company*. Oxford University Press, New York, NY, 1995.

Nonaka, I. “A Dynamic Theory of Organizational Knowledge Creation.” *Organizational Science*, 5:1 (1994): 14–37.

Schultze, U., and D. E. Leidner. “Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions.” *MIS Quarterly*, 26:3 (2002): 213–242.

Seebach, C. “Searching for Answers – Knowledge Exchange through Social Media in Organizations.” Proceedings of the 45th Annual Hawaii International Conference on System Sciences, 2012.

Siponen, M. T. “Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods.” *Information and Organization*, 15:4 (2005): 339–375.

Skeels, M., and J. Grudin. “When Social Networks Cross Boundaries: A Case Study of Workplace Use of Facebook and LinkedIn.” In Proceedings of GROUP’09, May 10–13, 2009, Sanibel Island, Florida, USA, 2009, 95–103.

Stenmark, D. “Information vs. Knowledge: The Role of Intranets in Knowledge Management.” In Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2002.

Tanriverdi, H. “Information Technology Relatedness, Knowledge Management Capability, and Performance of Multibusiness Firms.” *MIS Quarterly*, 29:2, (2005): 311–334.

Vodanovich, S., Sundaram, D., and M. Myers. “Digital Natives and Ubiquitous Information Systems.” *Information Systems Research*, 21:4 (2010): 711–723.

Wasko, M. M., and S. Faraj. “‘It is What One Does’: Why People Participate and Help Others in Electronic Communities of Practice.” *Journal of Strategic Information Systems*, 9:2–3 (2000): 155–173.

Wasko, M. M., and S. Faraj. “Why Should I Share? Examining Social Capital and Knowledge Contribution in Electronic Networks of Practice.” *MIS Quarterly* 29:1 (2005): 35–57.

Wenger, E. “Knowledge Management as a Doughnut: Shaping Your Knowledge Strategy through Communities of Practice.” *Ivey Business Journal*, 86:519 (2004): 1–9.

Yin, R. K. *Case Study Research*. SAGE Publications Ltd., Thousand Oaks, 2003.

FIGURES AND TABLES

Table 1. Knowledge protection challenges and special characteristics of SM as a new form of media

Knowledge protection challenges	**Characteristics of SM as a new form of media**
Information security challenges • Identity theft, scams, and phishing (Gross and Acquisti 2005; Malik and Malik 2011) • Disclosure of confidential information (Blakley et al. 2001; Skeels and Grudin 2009)	• *Information distribution speed* • *Blurry audience* • Merging of private and professional identity (Dhillon and Blackhouse 2001; Kuikka and Äkkinen 2011; Light et al. 2008) • *Easily collectible information* • *Generation transition*
Reputation challenge (Blakley et al. 2001; Aula 2010; Kuikka and Äkkinen 2011)	

Management challenges
• Crossing boundaries with SM (Skeels and Grudin 2009)
  • Communicate with customers/peers (Kuikka and Äkkinen 2011)
  • *Collect information about company*
• Legitimacy of using SM at workplace (Skeels and Grudin 2009)	

Table 2. Questions arising from and helping to respond to knowledge protection challenges

Question	**Examples of related knowledge protection challenges**
What role does SM play in the company?	Crossing boundaries with SM, Legitimacy of using SM at the workplace: Does the company want to use SM in its operations, e.g., to communicate with customers?
What kind of information can be shared in SM?	Disclosure of confidential information, Reputation challenge: Is there certain information that should or that cannot be shared, e.g., because of either improving or harming the company's reputation, or because of revealing information the company does not want to share?
Who is allowed to share information in SM?	Legitimacy of using SM at the workplace: Is SM use allowed or forbidden, is it restricted to only certain persons?
With whom is one allowed to share information in SM?	Disclosure of confidential information, Reputation challenge, Crossing boundaries with SM: Can every employee share information with customers, or just specifically assigned employees? Is there information that can be shared e.g., with colleagues, but not with people outside the company?
As to whom is one allowed to share information in SM?	Communicate with customers and peers: When sharing information with e.g., customers, should employees take the role of a representative of the company or can they share information as a private person, too?
When is one allowed to share information in SM?	Legitimacy of using SM at the workplace: If SM is not a tool used by the company, are employees allowed to use SM at the workplace?
Is one sharing information with whom they think they are?	Identity theft, scams, and phishing: Does someone try to get information from employees under another person's identity? Are employees aware of who has access to information they shared in SM?
Who is responsible for SM in the company?	Management challenges: Are responsibilities concerning SM clear in the company? Who is responsible for answering these SM-related questions?

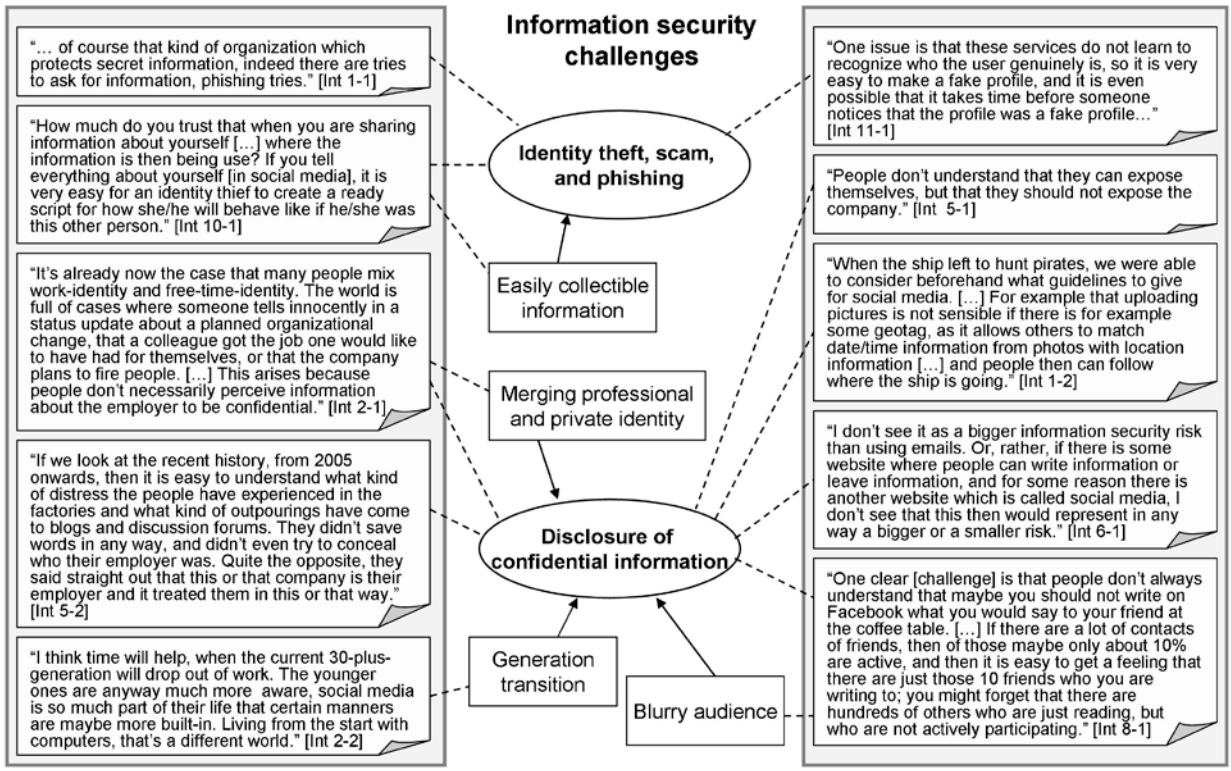

Figure 1. Information security challenges of SM.

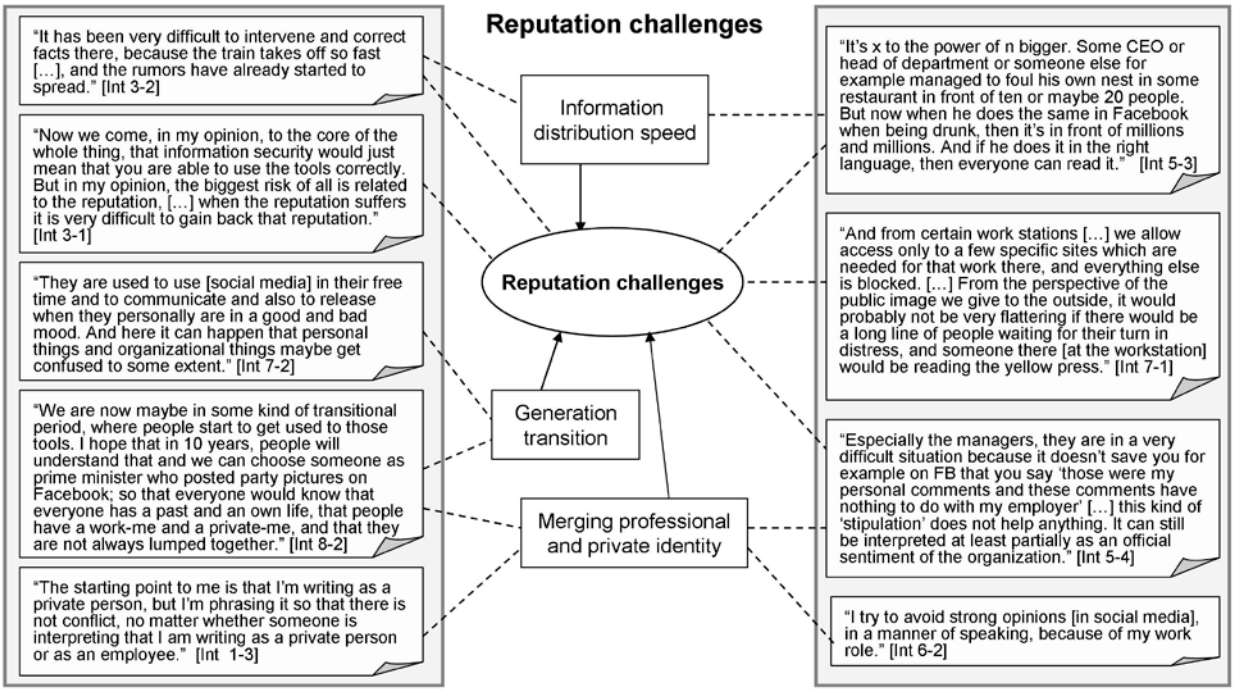

Figure 2. Reputation challenges of SM.

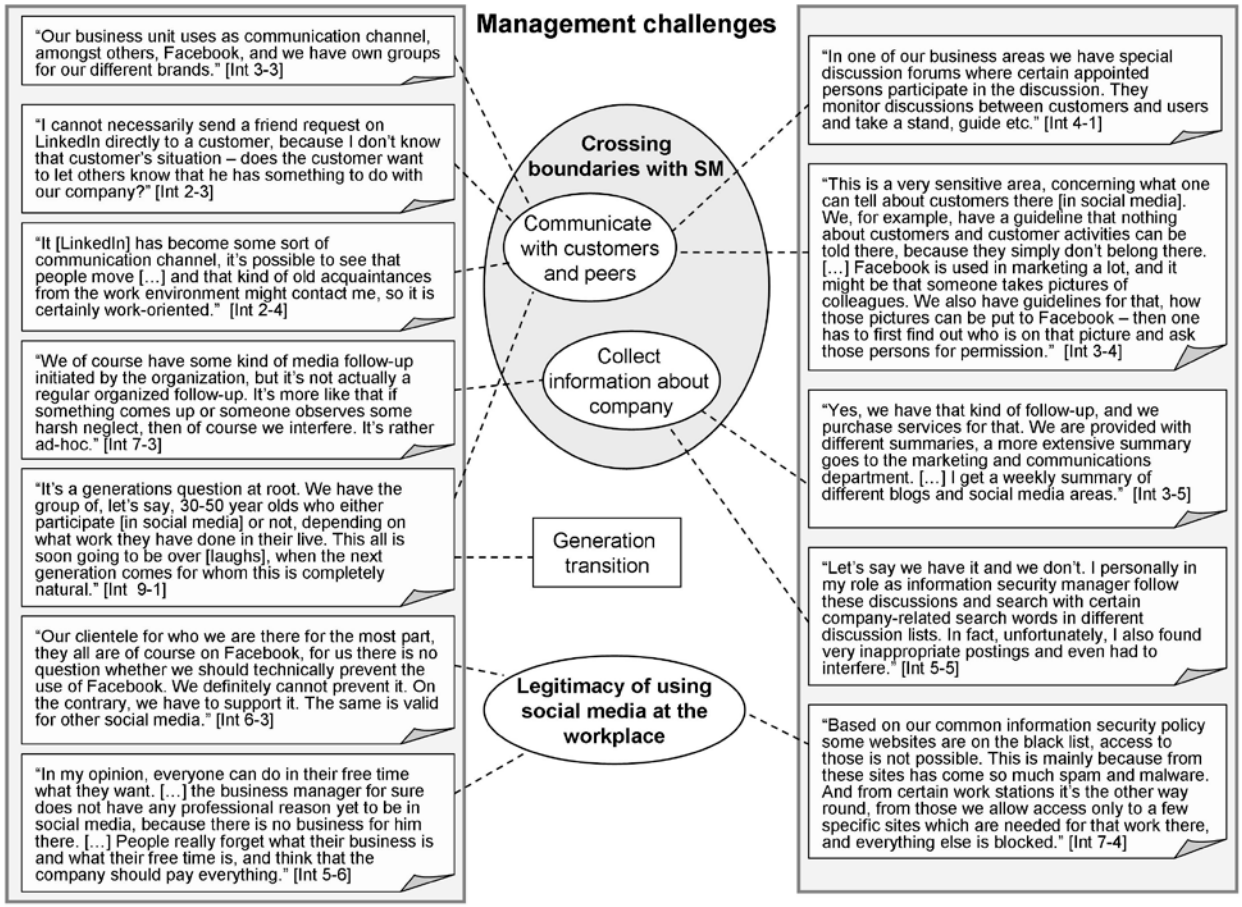

Figure 3. Management challenges of SM.

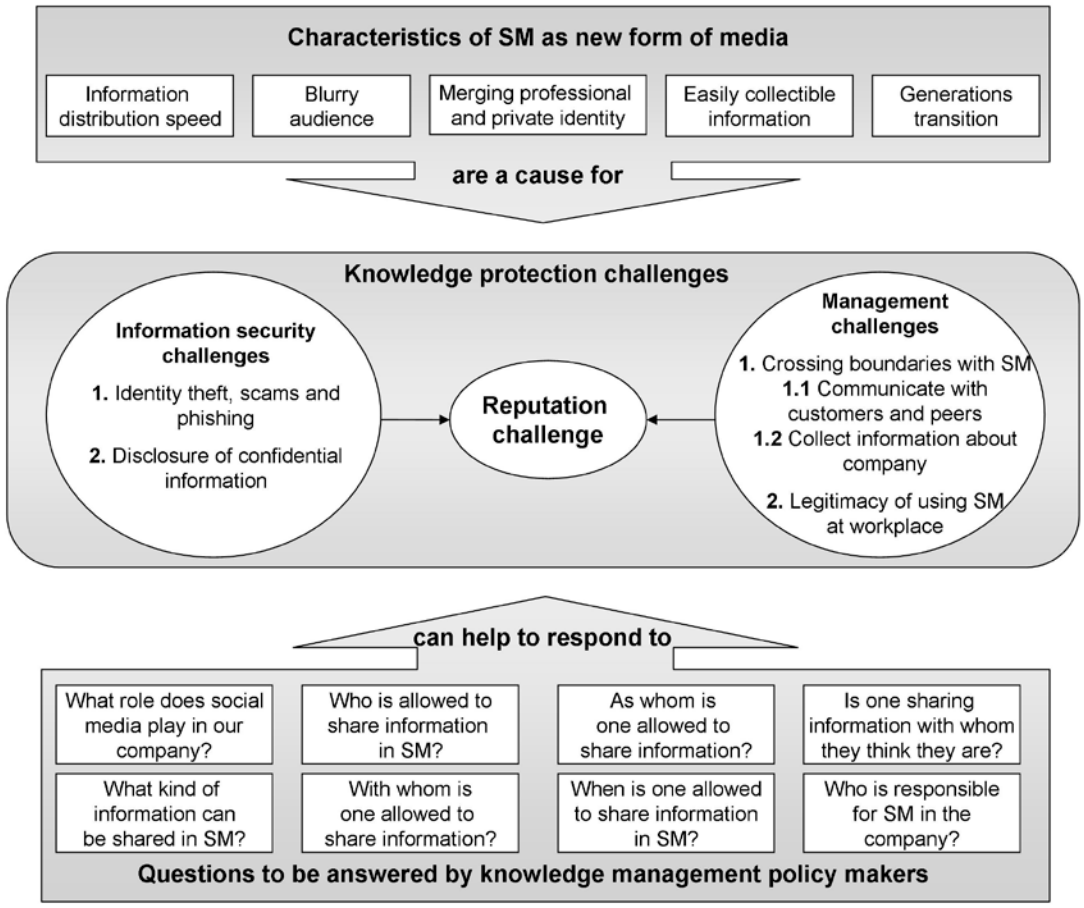

Figure 4. Framework of knowledge protection challenges arising from SM as a new form of media.