Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2012 Proceedings

European Conference on Information Systems (ECIS)

5-2-2012

# INFORMATION SECURITY CHALLENGES OF SOCIAL MEDIA FOR COMPANIES

Riitta Hekkala
*University of Oulu*

Karin Väyrynen
*University of Oulu*

Timo Wiander
*University of Oulu*

# INFORMATION SECURITY CHALLENGES OF SOCIAL MEDIA FOR COMPANIES

Hekkala, Riitta, Department of Information Processing Science, University of Oulu, 90014 FINLAND, riitta.hekkala@oulu.fi

Väyrynen, Karin, Department of Information Processing Science, University of Oulu, 90014 FINLAND, karin.vayrynen@oulu.fi

Wiander, Timo, Department of Information Processing Science, University of Oulu, 90014 FINLAND, timo.wiander@oulu.fi

## Abstract

*For companies and their employees, social media allows new ways to communicate with customers and colleagues. Vast amounts of information are being exchanged in social media. Information is a highly valuable asset, and therefore questions concerning information security become more and more important. Companies are becoming increasingly worried about information security in social media, but so far, this issue has not been studied. The present research closes this gap by studying the information security challenges social media represents for organizations. The research was conducted as a qualitative multiple case study for which information security managers from eleven public and private companies in one European country were interviewed. The study has three main findings. First, challenges arising from employees' actions or unawareness in social media (especially reputation damage) seem to represent bigger threats to information security than threats caused by outside attacks. Second, the confusion of private and professional roles in social media represents an information security risk, and distinguishing between these roles becomes more difficult the higher an employee's position in the company. Third, communication with employees and colleagues represents an information security challenge especially when communication is not steered by the company. Implications for research and practice are discussed.*

*Keywords: Social media, Information Security, Case study.*

# 1 Introduction

Information and communication technology (ICT) has long been a part of everyday life and plays an important role in organizations. Information technology (IT) offers organizations a large number of different opportunities and has, for example, continually increased innovation possibilities and opportunities for the creation of competitive advantage (Mata et al., 1995; Melville et al., 2004). Different kinds of information systems have been seen to be channels for humans to build identities, coordinate their relationships, and make sense of their environment among other things (Lamb and Kling, 2003). To date, social network sites have become an important and crucial part of daily communication practices for millions of people cf. (Facebook, 2011). Though social media is seen as a new means to communicate and collaborate, the concept of social media has its origins over 65 years ago when Bush (1945) expressed the idea that interconnections between computer systems may bring improvements to organizations' operations. Lately, the use of social media in organizations has become more popular (Light et al., 2008; Kuikka and Äkkinen, 2011). Social networking has become a 'hot' topic for academic researchers and business people alike (Light et al., 2008). An interesting question concerning social media has been asked by the popular press (Everett, 2010): is social media an opportunity or a risk? Previous research has focused on how companies can use social media in their business operations (e.g. Skeels and Grudin, 2009; Aula, 2010) and on the challenges organizations face in social media adoption (e.g. Kuikka and Äkkinen, 2010). Acquisti and Gross (2006) took Facebook as an example in raising privacy concerns based on Facebook's vast memberships, its unique and personally identifiable data, and the access it allows to information revelation behaviour of millions of users. On the one hand social networks offer new opportunities for interaction and communication, but on the other hand also raise new privacy concerns. Privacy in growing social networks has been seen as a challenge by Malik and Malik (2011) as well. Considerable amounts of information are exchanged between and within organizations and individuals using social media. This information itself is an asset of high value, and is therefore a key reason for why information security is becoming an increasingly important matter of interest (Dhillon and Backhouse, 2001; Siponen, 2005).

Information security has become a growing concern for companies by the advent of social media. New technologies for collaboration and interaction have increased the possibilities for information sharing. Although online communication has become very popular and has become the way to maintain social relationships, it has also highlighted the adverse effects on human behaviour. For companies, it would be important to get an understanding of whether and how social media represents a threat to information security in order to be better able to plan their appearances in and policies concerning social media. So far, research did not address this problem. This represents a clear research gap. The present research attempts to close this gap by asking the research question "*What are the information security challenges concerning social media for organizations?"* and answers this question by interviewing eleven information security representatives of different organizations.

The paper is organized as follows. In Section 2, we review the literature relevant to this study. Section 3 outlines the research methodology including research setting, data collection and analysis. The fourth section presents the findings of our qualitative analysis. In Section 5, we discuss the theoretical implications of our findings. We conclude our study with a summary of our contributions, implications for practice, research limitations and suggestions for future research.

# 2 Literature Review

Social media is defined by Kaplan and Haenlein (2010) 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'*. Trends suggest that social networking websites are becoming

more common and important for individuals (Szwedo et al., 2010), and recently also for organizations (Light et al., 2008; Kuikka and Äkkinen, 2011). Previous research has studied the roles of, and challenges posed by, social media to individuals and organizations from a number of perspectives. Next, we will briefly review past research on the roles and challenges of social media, followed by a review of information security challenges for organizations concerning social media.

## 2.1 Role and challenges of social media use in organizations

To date, there have been different ways to analyze the phenomenon of social media. Different blogs have been written about social media related topics, for example, about what motivates people to participate in social media (e.g. Nuxoll, 2010). Privacy issues and friending (Donath, 2007), as well as how social media is integrated into people's everyday lives (Hargittai, 2007), have been discussed. Skeeps 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 or customers or co-workers). They further discussed that questions concerning the *legitimacy of using social media at the workplace* and the *mixing of private and professional personas*, as well as *tensions over disclosing confidential information* can represent challenges for companies who intend to use social media. Also Light et al. (2008), when studying how social media plays a role in networking for both individuals and organizations, pointed out that Facebook accelerates the merging of people's work life and home life, making these different roles more public and more difficult to manage. In addition, they pointed out that for many companies, social networking technology is used in their *marketing efforts*, e.g. to communicate with customers and to attract new business. Kaplan and Haenlein (2010) studied how social media can be leveraged by organizations in form of collaborative project, blogs, social networking sites, virtual game worlds, and virtual social worlds. They advised companies to remember that the integration of social media 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. Aula (2010) studied the role of social media as a *reputation risk* when using it for corporate communication, and points out that in terms of reputation management it is important to remember that social media content cannot be controlled in advance, and that content cannot be managed in the same way as, for example, TV and newspapers. In addition, the role of social media concerning an individual's reputation has been studied (Madden and Smith, 2010).

A recent study by Kuikka and Äkkinen (2011) on challenges social media represents for companies identified internal and external challenges similar to those identified by the above presented authors' findings. Internal challenges concern *resource challenges* (e.g. how employees use their work time), *ownership challenges* (who is responsible for social media in the company), *authorization challenges* (i.e. who is allowed to contribute to social media), *attitude challenges* (i.e. employees' attitude towards the use of social media), and *economic challenges* (i.e. costs related to implementing a social media strategy). External challenges concern *reputation challenges*, *legal challenges*, and *identity challenges* (i.e. the question of distinction between a person's professional and private identity).

## 2.2 Information security challenges in organizations related to social media

The term "information security" is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **integrity** (which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity), **confidentiality** (which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information), and **availability** (which means ensuring timely and reliable access to and use of information) (Legal Information Institute, 2011).

Information security is required, because the application of technology to information creates risks. Information might be improperly disclosed, modified in an inappropriate way, or destroyed and lost

which can result in, for example, financial losses and damages to reputation (Blakley et al., 2001). As discussed above, in the context of social media, especially the improper disclosure of information, i.e. confidentiality, is a risk for companies. Malik and Malik (2011) found that large-scale social networks pose privacy challenges due to the large amount of possibly sensitive and private information stored in those networks. They argued that disclosing personal information in social networks is a double-edged sword: on the one hand, disclosure is a plus or even must if people want to participate in social networks. On the other hand, disclosing personal information can invite malicious attacks like *phishing, spamming, distribution of malware, making identity theft easier, and scams*. Gross and Acquisti (2005) argued that *lacking privacy* in social media networks increases the risk of identity theft. They found that personal data is generously provided in Facebook (one of the largest social media networks today) and that this enables online and physical *stalking*, *data re-identification* (i.e. linkage of datasets without explicit identifiers such as name and address to datasets with explicit identifiers through common attributes), *blackmailing*, and *social engineering*.

Zheleva and Getoor's (2009) study showed that homogenous groups in social media (e.g. groups focusing on a certain area of interest) can *leak a significant amount of personal information*, and that privacy can be better preserved if one does not join those groups. Interestingly, Acquisti and Gross (2006) did not detect a relation between participants' reported privacy attitudes and their likelihood of providing certain information. They suggested that privacy attitudes have some effect on whether a person joins a social network in the first place, but after a person has joined, there is very little marginal difference in information revelation across groups. They further suggested that this might be the result of perceived peer pressure or herding behaviour. It has been highlighted that users might underestimate the dangers of publicly posted materials on the web (Donath, 2007; Jagatic et al., 2007; Light et al., 2008; Allen, 2011). Light et al. (2008) argued that users trusted in the privacy of social network sites, assuming these sites were 'closed worlds', and as a consequence published, for example, provocative material. The dilemma seems to be that the protection of privacy has changed because of technology, and nowadays people even share intimate thoughts with anonymous Internet users. This same phenomenon is becoming a significant risk in organizations. According to Allen (2011), possible threats and consequences for the people who share information too freely include privacy risks, being rejected when applying for a job, being fired due to inappropriate posts in social media, and posts leading to threats. They further argued that for the organization those people work in, too free sharing of information can result in security risks. Dhillon and Backhouse (2000) have stated that computer security in itself is not a technical problem; it has social and organizational dimensions that involve people who operate these technical systems. They suggested that information security principles need to be expanded to incorporate responsibility, integrity of people, trustworthiness and ethics into the classic confidentiality, integrity and availability (CIA) triad model. Furthermore, they stated that information security should not simply be viewed as means of protecting physical assets alone. By taking individuals and their social relationships into account, the protection level should be expanded (Dhillon and Backhouse, 2001). This protection should cover the different roles (aka working role vs. private role), use of different user names and passwords in different domains (private and work related), and guidelines and policies how to behave in social media to name just a few.

In summary, the most prevalent challenges for information security caused by social media seem to be related to data integrity and confidentiality (leaking information by accident, phishing, identity theft, scams, spam, malware, reputation damage) and to the different roles of social media in the company (private vs. professional identity, networking, marketing tool).

# 3 Methodology

The present research was designed and conducted as a multiple-case case study. Yin (2003: 13) stresses that the case study is 'an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident'. A case study can involve single or multiple cases and many levels of analysis. The

main characteristics of a case study are that the aim of the research is to explore certain phenomena and to understand them in a particular context, and that the researcher uses multiple methods for collecting data. However, Yin is writing from a positivist perspective – what he means by 'phenomena' is not what an interpretive researcher means. Robey et al. (2000: 133) maintain that 'case studies provide the greatest detail on the role of experience'. Eisenhardt (1989: 548) also recommends the use of the case study approach if 'little is known about a phenomenon, current perspectives seem inadequate because they have little empirical substantiation, or they conflict with each other or common sense'.

Four types of analytical generalisation from interpretive case studies are suggested by Walsham (1995): development of concepts: a concept can be part of several concepts, propositions and world views which form theories; generation of theory: a framework could suggest areas for theoretical development; drawing of specific implications: the implication can provide a good description of the case study which was investigated; and contributions of rich insight: including insights/results that are not easily categorised, for instance as concepts or theories. The information security threats related to social media from the perspective of an organization are yet unexplored, and therefore the case study offers a suitable research method for the present study. Walsham (1995) highlights that interviews are still an important data source in case study, since they, for example, enable researchers to step back and examine the interpretations of their fellow participants in some detail (Walsham, 1995).

The **research setting** of the study was the following: this study is part of a broader research initiative whose aims were to study 1) the development of methods for creating organization specific information security policies, 2) security integration with different information systems and software development methods, and 3) increasing employees' compliance with information security instructions through well planned education and training. As part of this broader research initiative, the present research concentrated on the most important challenges which social media represents to information security. Before the actual research was conducted, we made a pilot case study (see Yin 2003: 78ff.) with eight specialists in the social media and information security fields. Based on these interviews, we aimed to identify the topics which needed further analysis. For the actual research, informants were selected based on their vast experience with information security. Interviewees wanted to be kept anonymous. We conducted interviews in organizations of different sizes (SME to large multinational organizations), and in both the public and private sector in one European country, to get a broader understanding of the issue under study. The interviews were conducted in the Armed forces, an information security consulting service company, two telecommunications companies, a company in the pulp and paper industry, the Parliament, the Border Guard, a software vendor, an airport service provider, a logistics company, and the Security police.

During the **data collection** in the actual research, we conducted eleven semi-structured interviews (see Myers and Newman, 2007) in January and February 2011. Interviews lasted from 30 to 59 minutes (on average 47 minutes), which equals a total of 88 pages of transcribed text. Questions asked for this study were, amongst others, "What kind of information security threats does your organization or line of business encounter regarding social media?", "Have you had any kind of cases where social media has been a reason for data leakage, reputation risk, or any other information security threat?" and "Do you know other organizations where social media has caused an information security threat?" 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, analysing within-case data, searching for cross-case patterns, shaping hypothesis, and enfolding literature. In the data analysis, we used the challenges we identified in relation to information security in Section 2.2. as pre-nodes (i.e. malware, spam, scams, phishing, identity theft, leaking information, reputation damage, networking, confusion of private and professional identity) and analyzed whether and how those are seen as representing challenges to information security for companies. In the analysis, we identified a number of additional information security challenges for companies in relation to social media (i.e. untrusted applications, unsafe internet connection, audience blur, and social media as "the next media").

# 4 Findings

This section discusses what the most important challenge types and risks in social media from the information security's point of view are. Our interviews revealed that the major challenges are 1) outside attacks on employees or the company, 2) challenges caused by employee's actions or unawareness, and 3) challenges related to roles (see Table 1). Newly identified challenges not yet identified in previous research are denoted in italic letters in Table 1. We will add information about which interview the presented information is taken from by adding "Int" and a number from 1 to 11, e.g. "(Int 5)" for Interview 5. Information security risks will be denoted in bold letters, and observations related to these risks will be pointed out in bold and italic letters in Sections 4.1 – 4.3.

| **Challenge type** | ***Information security risks*** |
|---|---|
| Outside attacks on employees / company | Malware, Spam, *Untrusted applications, Unsafe Internet connection (remote work)* |
| Challenges arising from employees' actions / unawareness | Scams, Phishing, Identity theft, Leaking information (*intentionally* or *by accident*), *Audience is blurring,* Reputation damage |
| Challenges related to roles | Social media as networking tool (customer communication or keeping network of professional peers) , Confusion of private and professional identity, *Social media as 'the next media'* |

*Table 1. Social Media Challenge Types and Information Security Risks*

## 4.1 Information security challenges from outside attacks on employees / the company

The risks related to outside attacks on employees or the company mentioned by the interviewees were malware, untrusted applications and insecure Internet connection. The danger of **malware** being distributed in social media was mentioned by several interviewees (Int 10): *"And of course the applications are not perfect, there may be vulnerabilities or bug issues which can cause surprises…that some hacker can publish some fun, nice extra application, which is some malware…"* One particular challenge related to malware are certain Facebook applications. These applications can transform into malware after the user has given the application permission to access certain user data, meaning that that malware then has access to that same data (Int 3): "*For example, on Facebook where users give different applications permission to do something. The applications are not static. There are some examples where the function of an application has changed radically, but the permission of the user exists, and in a worst case the application will change to malware."* Traditionally, companies control rather well which applications can be installed by whom and on which computer. Social media changed this, however, as it allows everyone to install applications in their Facebook profiles, which the organization does not have an influence on (Int 8). As one countermeasure against malware and **spam**, some companies deny access to certain social media sites (Int 7): *"Based on a common information security policy, some sites are on a black list, so it's not possible to access these sites. This is mainly because there have been problems with lots of spam or malware from those sites."* Another challenge identified was that people log in to different services (e.g. **untrusted applications**) using other accounts such as Facebook accounts (Int 9): *"For example, you can log in to different services x, y, z using your FB account data. There are two problems: a) your FB account is going to be more vulnerable, because you have several services you can log in to using the same account… b) another issue is that I can put the Facebook logo on my service page [laughing], and say 'log in using your Facebook account', and then a little window opens which says 'use your FB account login data', and now I stole them [the login data]."* One risk related to **unsafe internet connection** was 'remote work', i.e. where employees work from home using unsafe internet connections.

Several interviewees, however, pointed out that these ***technical threats might not be very severe threats*** from an information security perspective (Int 8): "*The starting point for information security is*

*that social media is not an information security problem, we have good tools that take care of cases of malware and similar things, and we have instructions for how one should behave on the internet and in social media. So in that sense social media is not a problem."* Another interviewee pointed out that in his opinion, malware is not really a good reason for preventing the use of social media in a company (Int 8): *"I have myself been wondering about some colleagues who have a very negative attitude towards social media, and who often use then the malware-card as a reason, but in my opinion this should be tackled in a different way."* One interviewee did not think that social media would increase the malware problems in his company (Int 4): "*The same kind of malware is also elsewhere. […] I don't really know whether this increases the problem of malware in the company."*

## 4.2 Information security challenges from employee's actions/ unawareness

Several risks identified could be lead back to employees' actions in social media, which often are caused by unawareness of certain threats or characteristics of social media. These risks were related to phishing, identity thefts, leaking information, reputation damage and blurring of the audience in social media. Risks related to scams and phishing were greater in those organizations which clearly have confidential data to protect. Threats related to **scams**, **phishing** and **identity thefts** were seen as risks for similar reasons. In both cases, someone makes use of information they tricked out of the victim or collected about the victim, and social media is seen as a way to easily collect information about others; it is easy to open a fake account and impersonate someone else. Another user then might allow this "fake" person access to their data without realizing that this other person is a defrauder (Int 11): *"One issue is that these services do not learn to recognize who the user genuinely is, so it is very easy to make a fake profile, and it is even possible that it takes time before someone notices that the profile was a fake profile…"* Another interviewee explained this risk similarly (Int 10)*: "How much you trust that when you are sharing information about yourself, what the purpose is, where the information is being used. If you tell everything about yourself there, it is very easy for the identity thief to create a ready script for how she/he will behave like he/she was this other person."*

**Information leakage** was seen as a risk from a number of different perspectives. First of all, employees can **leak information by accident** in social media. This can happen, for example, when writing a blog, or when logging in to different services using, for example, Facebook accounts (see Section 4.1). One interviewee gave an example where an employee posted information on the progress of an international operation in a blog, telling what events are going to happen next. As a result, for the next operation the company gave guidelines for the use of social media (Int 1): *"When the ship left to hunt pirates, we were able to consider beforehand what guidelines to give for social media. […] For example that uploading pictures is not sensible if there is for example some geotag, as it allows others to match date/time information from photos with location information […] and people then can follow where the ship is going."* Second, employees can **leak information intentionally**, for example because of being unsatisfied with their employer (Int 5): *"If we look at the recent history, from 2005 onwards, then it is easy to understand what kind of distress the people have experienced in the factories and what kind of outpourings have come to blogs and discussion forums. They didn't save words in any way, and didn't even try to conceal who their employer was. Quite the opposite, they said straight out that this or that company is their employer and it treated them in this or that way."* One reason for problems concerning information leakage was seen to be the ***trust people put into their networks***. Several interviewees thought that people have excessive trust of their networks, and people are giving too much information or facts about themselves, and their organizations. The information security managers also thought that especially the hype surrounding social media encourages excessive trust. In addition, social media makes it difficult to control who gives information about the organization (Int 7): *"[…] and there have been certain rules concerning communication, and now this [social media] allows deviance from that."*

Another problem related to information leakage and information sharing in general seems to be that often, the **audience is "blurring"**, people are not conscious about the number of people who actually

can see their postings. Several information security managers were worried about this (Int 8): *"One clear [challenge] is that people don't always understand that maybe you should not write on Facebook what you would say to your friend at the coffee table. […] If there are a lot of contacts of friends, then of those maybe only about 10% are active, and then it is easy to get a feeling that there are just those 10 friends who you are writing to; you might forget that there are hundreds of others who are just reading, but are not actively participating."* However, some interviewees did not see social media as any bigger risk to information security than other media (Int 6): *"I don't see it as a bigger information security risk than using emails. Or, rather, if there is some website where people can write information or leave information, and for some reason there is another website which is called social media, I don't see that this then would represent in any way a bigger or a smaller risk."*

One big concern related to social media was **reputation risk and the control of reputation**. One interviewee thought that social media is not a bigger risk than the use of email. The most central risk was seen to be how to 'sustain' one's reputation (Int 3): *"Now we come, in my opinion, to the core of the whole thing, that information security would just mean that you are able to use the tools correctly. But in my opinion, the biggest risk of all is related to the reputation. If some malware manages to get into your network, then it can do something there, impede the work or interrupt it. But if we think about the reputation risk, when the reputation suffers it is very difficult to gain back that reputation."* Some companies deny access to social network sites, amongst other reasons, to prevent bad publicity (Int 7): *"And from certain work stations […] we allow access only to a few specific sites which are needed for that work there, and everything else is blocked. […] From the perspective of the public image we give to the outside, it would probably not be very flattering if there would be a long line of people waiting for their turn in distress, and someone there [at the workstation] would be reading the yellow press."* Especially difficult in relation to reputation is the ***speed of information distribution*** in social media (Int 3): *"It has been very difficult to intervene and correct facts there, because the train takes off so fast […], and the rumors have already started to spread."* In addition, the posting of employees' 'inappropriate' private opinions and pictures in social media was seen as a possible threat to the organizations' reputation. This brings us already to the third category of challenges, including the difficulty of distinguishing between private and professional identity in social media.

## 4.3 Role-related information security challenges

Social media played different roles in different companies. It was used by several companies as a way to **keep in contact with different types of networks**. For one, social media was used to ***communicate with customers*** in form of blogs or special interest groups. In this connection, one challenge is how to define which of the employees is actually allowed to interact with others in social media (H1): *"You can never go back and say '… but I only commented as private person!' Here also the organization has to make clear who is really allowed to write as [a representative of] our organization, if our organization would have some [social media] website."* Second, social media was used by employees to keep in contact and collaborate with their colleagues. Especially LinkedIn was mentioned repeatedly as a tool to ***keep a network of professional peers*** (H2): *"It [LinkedIn] has become some sort of communication channel, it's possible to see that people move […] and that kind of old acquaintances from the work environment might contact me, so it is certainly work-oriented."*

One big challenge related to several of the above identified challenges was the **confusion of private and professional roles and identity** in social media. Several interviewees thought there is the danger that ***employees' private statements would be interpreted as statements of the company***. Especially with younger employees, the danger of confusing private and professional personas might be higher (Int 7): *"They are used to use [social media] in their free time and to communicate and also to release when they personally are in a good and bad mood. And here it can happen that personal things and organizational things maybe get confused to some extent."* In addition, some interviewees thought that mixing private and professional personas is a ***bigger problem for people on a higher hierarchy level*** than for those on a lower level, as people in higher positions or people who are well known are

stronger connected to the company in people's minds (Int 5): *"Especially the managers, they are in a very difficult situation because it doesn't save you for example on FB that you say 'those were my personal comments and these comments have nothing to do with my employer' […] this kind of 'stipulation' does not help anything. It can still be interpreted at least partially as an official sentiment of the organization."* Several interviewees mentioned that they actually adapt their communication in social media to their work role, to prevent a conflict between the private and professional roles (Int 1): *"The starting point to me is that I'm writing as a private person, but I'm phrasing it so that there is not conflict, no matter whether someone thinks that I'm writing as private person or as an employee."*

There was disagreement about the **role social media plays compared to other forms of media**, i.e. whether social media really differs that much from other, more traditional, media. Some interviewees thought that social media represents other challenges for information security than previous media, e.g. concerning the distribution of information (Int 5): *"And another issue is that it [social media] is so indefensible and completely out of control, people can do things there by accident which they regret the rest of their life. […] And it is irreversible once it's done, it cannot be corrected easily, if at all."* The challenges related to social media were also seen to be in something like a transitional period, as one interviewee said (Int 9): *"It's a generations question at root. We have the group of, let's say, 30-50 year olds who either participate [in social media] or not, depending on what work they have done in their live. This all is soon going to be over [laughs], when the next generation comes for whom this is completely natural."* Another interviewee explained that he trusts younger people more in that they know how to behave in social media, as they grew up with social media and therefore might be better able to evaluate the consequences of posting in social media than older generations (Int 2). However, not all interviewees saw social media to be different from other media, but instead saw it as "simply the next media" which does not differ much from other media (Int 8): *"In my opinion, if you need specific guidelines for social media, then your information security guidelines have been bad. Social media basically is just a new service on the internet for which the old guidelines still hold."* Similarly, one interviewee saw social media just as another way to communicate (Int 9).

# 5 Discussion

Next, we discuss our main findings. We found that there are different types of challenges and threats to information security present in social media. Information security challenges arising from outside attacks on employees, which as a result can have information security impacts on the company, are malware, untrusted applications, and insecure internet connections. Information security challenges arising from actions of the employees in social media include scams, phishing, identity theft, leaking information (intentionally or by accident), reputation damage, and the fact that audience is blurring in social media. Challenges related to roles refer to threats arising from the role social media plays for networking in the company, confusion of private and professional roles and identity, and the role of social media as 'the next media'. Here, we want to discuss some of these challenges in more detail.

A substantial amount of past research on information security challenges of social media concentrated on those arising from outside attacks, i.e. problems arising through malware, spam and so on (e.g. Malik and Malik, 2001; Gross and Acquisti, 2005). One important finding of the present study is that social media does not seem to represent much bigger information security threats arising from outside attacks than other types of media. There was vast agreement on that malware, spam, untrusted applications and unsafe internet connections can be tackled with technical means rather well nowadays, and that these are bad reasons for prohibiting the use of social media at the workplace. We also found that social media makes it more difficult for companies to control what kind of applications get access to the company's computers, as social media allows employees to install applications *inside* social media, from where these applications can get access to company data. However, based on the findings of our study, the information security threats related to employee's actions in social media seem to represent a much bigger challenge, especially in terms of reputation damage. This is a new finding which has, to our knowledge, not yet been taken up in the context of social media. Blakley et

al. (2001) pointed out that information security breaches in general can result in reputation damage. Our study showed that social media represents an even bigger threat to reputation than other, more traditional media, because people might have too much trust in their social networks, because information travels so much faster in social media, and because employees might not always be aware of just *how many* people actually have access to what those employees write in social media. Reputation risk can be seen from two different perspectives. Aula (2010) discussed reputation risk from the perspective where the company willingly engages in social media e.g. to advertise their company, or to interact with their customers. Our study, on the other hand, showed that reputation risk also arises when employees share information about the company in social media, either by accident or intentionally, without the company steering it. In fact, Kuikka and Äkkinen (2010) expected companies to be concerned about employees posting things in social media which would have a negative effect on the company's reputation, but their study did not support this expectation. Our findings differ from Kuikka's and Äkkinen's (2010) finding, as we managed to show that this is indeed a concern for companies, especially from an information security perspective.

Skeels and Grudin (2009), when studying the workplace use of Facebook and LinkedIn, found that people often mix private and professional personas, and that they then adjust posts for a broader audience (so that it is suitable for family, friends, and co-workers). We also identified this behavior in our study but found that, from an information security perspective, this is actually a desirable behavior. Where employees adjust the content of their messages to a broad audience, it suggests that those employees are much better aware of the threats related to accidentally leaking information. A much bigger problem represent those employees who are not adjusting the content of their messages because they forget who else can read their postings. Interestingly, we found that this need to adjust messages for a broader audience is also seen as being dependent on the employee's position. The higher the employee's position, the less likely it is that a distinction between private and professional identity in social media would be possible. For example, a company's CEO who is present in the media is often automatically connected to that company wherever he appears. For that kind of CEO it is almost impossible to appear as private person whose comments have nothing to do with his employer. On the other hand, if a programmer in a 1000-person-company shares his political views on Facebook, it is rather unlikely that this would be interpreted as his employer's official political view.

Our findings showed that social media networks are used by companies and their employees to communicate and collaborate with their colleagues and customers, i.e. to maintain certain networks. Kuikka and Äkkinen (2011) found that in more traditional organizational information systems, people's network identities have been framed in the context of the organization, and that social media changed this by allowing employees to also communicate and collaborate with customers in their 'private roles'. Our study extends Kuikka's and Äkkinen's (2011) findings by showing that the mixing of private and professional roles when communicating and collaborating with customers and co-workers in social media is also a big challenge from an information security perspective. It seems that companies manage to ensure information security better in those cases where the company is actively steering and controlling this communication and collaboration, for example by defining who in the company is allowed to communicate with customers in social media as representatives of the company (in other words, where employees clearly know that they take a professional role in social media). However, as our study showed, a risk for information security represents the communication and collaboration that employees initiate and participate in independent of the company, where private and professional roles get confused, as discussed in more detail above. Interestingly, certain social media networks were mainly seen as "professional networks" (e.g. LinkedIn), while in other social media networks (e.g. Facebook) the distinction between private and professional role seemed more difficult. We found it interesting that the interviewees, which all were responsible for information security management in their companies, had very different attitudes towards social media and the possible threats to information security. While some thought that social media represents very specific challenges to information security, others did not see social media as a bigger risk than any other media.

# 6 Conclusion

The present research attempted to answer the question what the information security challenges of social media are for organizations. We want to emphasize **three main findings**. *First*, we categorized information security challenges into three types of social media challenges (outside attacks on employees/company, challenges arising from employees' actions/unawareness, and role-related challenges) and found that challenges arising from employees' actions or unawareness seem to represent bigger risks for information security than challenges caused by outside attacks. Especially reputation management seems to be a major information security concern of companies related to social media. *Second*, we found that confusion of private and professional roles represents an information security risk for collaboration and communication in social media network. We found that whether and how far a distinction can be made between private and professional roles and identity in social media heavily depends on an employee's position in the company. *Third*, we found that companies and employees use social media networks to collaborate and communicate with co-workers and customers. From the perspective of information security, this represents a challenge especially when communication and collaboration is initiated and participated in by employees without being steered by the company, as in those cases it is more likely that employees' private and professional roles get mixed. In addition to the theoretical implications which were presented in Section 5, our study has also **practical implications**. Given the very different types of challenges or threats for information security, social media should become part of companies' information security policy. However, because how much of a threat social media is seen as depends very much on personal experience and opinions of information security managers, companies should make sure these policies really are developed. Our study has **limitations**. The study was conducted in ten different companies in one country, and this country-specific context might have influenced how information security managers in general see information security risks arising from social media. **Future research** could study how these information security policies should be developed in practice and could take the results of our study, testing them in form of, for example, a quantitative study. In addition, it would be interesting to see whether certain findings of this study are dependent on the specific country-context, or whether these information security risks are seen to be the same in other country-contexts as well.

# References


Acquisti, A. and Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Privacy Enhancing Technologies. Lecture Notes in computer science, 4258/2006, 36-58.

Allen, J.P. (2011). Social Media Risks. The Latest Potential Disasters Outlined. http://www.jpedia.org/wp/archives/383. Accessed on 23rd May 2011.

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

Blakley, B., McDermott, E. and Geer, D. (2001). Information Security is Information Risk Management. In Proceedings of the 2001 workshop on New security paradigms (NSPW'01) (Raskin, V. and Greenwald, S.J. Eds.), p. 97-104, Cloudcroft, New Mexico, USA.

Dhillon, G. and Backhouse, J. (2000). Information System Security Management in the New Millennium. Communications of the ACM, 43(7), 125-128.

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

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

Eisenhardt, K.M. (1989). Building Theories from Case Study Research. The Academy of Management Review, 14(4), 532-550.

Everett, C. (2010). Social Media: Opportunity or Risk? Computer Fraud & Security, 6, 8-10.

Facebook (2011). http://www.facebook.com/press/info.php?timeline. Accessed on 30th May 2011.

Gross, R. and Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks. In Proceedings of ACM Workshop on Privacy in the Electronic Society (WPES'05) (Atluri, V., De Capitani di Vimercati, S. and Dingledine, R. Eds.), p. 71-80, Alexandria, Virginia, USA.

Hargittai, E. (2007). Whose Space? Differences among Users and Non-Users of Social Network Sites. Journal of Computer-Mediated Communication, 13(1), 276-297.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007). Social Phishing. Communications of the ACM, 50(10), 94-100.

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

Kuikka, M and Äkkinen, M. (2011). Determining the Challenges in Organizational Social Media Adoption and Use. In Proceedings of the 19th European Conference on Information Systems (ECIS'11), (Tuunainen, V.K., Rossi, M. and Nandhakumar, J. Eds.), paper 248, Helsinki, Finland.

Lamb, R and Kling, R (2003). Reconceptualizing Users as Social Actors in Information Systems Research. MIS Quarterly, 27(2), 197-235.

Legal Information Institute (2011). http://www.law.cornell.edu/uscode/44/3542.html. Accessed on 15th November 2011.

Light, B., McGrath, K. and Griffiths, M. (2008). More Than Just Friends? Facebook, Disclosive Ethics and the Morality of Technology. In Proceedings of the 29th International Conference on Information Systems (ICIS'08), paper 193, Paris, France.

Madden, M. and Smith, A. (2010). Reputation Management and Social Media, Report from the PewResearchCenter (http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx). Accessed on 30th Sept 2011.

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

Mata, F.J., Fuerst, W.L. and Barney, J.B. (1995). Information Technology and Sustainable Competitive Advantage: a Resource-Based Analysis. MIS Quarterly, 19(4), 487-504.

Melville, N., Kraemer, K. and Gurbaxani, V. (2004). Review: Information Technology and Organizational Performance: an Integrative Model of IT Business Value. MIS Quarterly, 28(2), 283-322.

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

Nuxoll, K. (2006). What Motivates People to Participate in Online Communities. http://www.newassignment.net/blog/kelly_nuxoll/dec2006/15/what_motivates_p.2006. Accessed on 27th May 2011.

Robey, D., Bourdeau, M.C., and Rose, G.M. (2000). Information Technology and Organisational Learning: a Review and Assessment of Research. Accounting Management and Information Tecnologies, 10(2), 125-155.

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

Skeels, M. and Grudin, J. (2009). When Social Networks Cross Boundaries: a Case Study of Workplace Use of Facebook and LinkedIn. In Proceedings of the ACM 2009 international conference on Supporting group work (GROUP'09), p. 95-104, Sanibel Island, Florida, USA.

Szwedo, D. E., Mikami, A.Y., and Allen, J.P. (2010). Qualities of Peer Relations on Social Networking Websites: Predictions From Negative Mother-Teen Interactions. Journal of Research on Adolescense, 21(3), 595-607.

Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. European Journal of Information Systems, 4(2), 74-81.

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

Zheleva, E. and Getoor, L. (2009). To Join or Not to Join: the Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles. In Proceedings of the 18th International World Wide Web Conference (WWW) (Quemada, J., León, G., Maarek, Y.S. and Nejdl, W. Eds.), p. 531-540, Madrid, Spain.