DEGREE PROJECT

Social Media Risk Management

& the impact on organization IT security

Malena Holmstedt

Information Security, master's level (120 credits)
2020

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY

Abstract

The purpose of this study was to investigate and try to describe how social media risk management is performed and what impact social media risk management could have on organizations IT security.

The outcome of this study is possible knowledge for researchers and for practitioners in the field, of how social media risk management was handled in some organizations in Sweden and what impact the chosen social media risk management could have on the IT security.

This study looked at social media risk management and what impact it could have on organizations IT security through prior studies done and through data collected from semi structured interviews and surveys.

Social media risk management was according to this study performed mostly reactive and a majority of the organizations did not have risk management specifically for social media. More organizations had a social media policy than performed risk management for social media.

The risk management for social media in the IT organizations in this study was described in the interviews as reactive due to several reasons: old systems that made it hard to be proactive, lack of time for prioritizing social media risks or risk management for social media was currently being worked on.

The proactive IT organizations described themselves to have a general security policy and risk management plans for basically everything.

Social media risks can lead to risks that impacts organization IT security. In the interview notes five quotes was found that could be considered to suit the risks themes found in prior studies.

Keywords: Information Security, IT security, Risk Management, Social Media Risk Management, Proactive Reactive Security

Acknowledgements

I would like to express my deepest gratitude to all the interview and survey participants for giving me of your valuable time and knowledge.

I would also want to express my sincere gratitude to my supervisor Abdolrasoul Habibipour and my seminar members for all your time and all your constructive feedback.

Last but not the least, a big thank you to my family, friends and classmates who kept motivating me and encouraging me to keep going when I felt like giving up.

You all made this thesis possible and for that I will forever be grateful.

Borlänge, June 2020

Malena Holmstedt

1 Table of Contents

Table of Figures

Table of Tables

1. Introduction

In this section the background of the research field is presented then the related work, the research gap, research questions, the purpose of the study, the research question and finally the delimitation of the study is explained.

1.1. Background

Social media is defined by Ellison & Boyd as: *"...the socio-technical dynamics that unfolded as millions of people embraced the technology and used it to collaborate, share information, and socialize."* [1, pp. 10-11]. Social media can be used by humans to exchange information or content, collaborate and a lot more and is described as something continuously changing because of the internet and the technology used for social media evolving constantly [2].

A study of the fastest growing organizations in the USA 2017, states that 92 percent of the organizations uses a LinkedIn account and 90 percent uses a Facebook account. It also states that 50 percent of the studied organizations did not have a social media policy written [3]. A social media policy should be in place to guide employees on what is appropriate behaviour on social media, but only 50 percent of employees in a study did know what specifically would violate the social media policy of the organization [4].

In another study 75 percent of the studied organizations social media policies did not give a definition of to whom or where the social media policy applies to, which may cause confusion of the intent or purpose of the social media policy [5]. An analysis of different threats of social media by Gupta, Thakral & Choudhury [6] shows that 70% of the threats of spam mail and phishing can be countered by educating the users. *"Effective protection is therefore achieved only through a holistic approach combining a secure technical system with individual security awareness."* [7, p. 5].

Social media can be used on organization computers or on employee devices used on the organization network. Social media should not be understated as an important factor for information communication for organizations but the benefit of it comes with risks [8] [9]. For example, a few of the social media risks are loss of information, loss of reputation, identity theft and technical risks like malware [10].

A risk is described by the ISO standard definition like*:" ... the possibility of an effect and, in particular, an effect on objectives*" [11, p. 882]. Information security risk management is about calculating how much risk the organization is willing to cope with against the cost of implementing security controls [12]. There are a lot of different techniques of carrying out risk management like for example: ISO 31000, ISO/IEC 27005, Octave Allegro and ERM.

Choi et al [13] example of proactive security countermeasures is for example a vulnerability management system or a patch management system. The function of proactive security countermeasures is to try to eliminate vulnerabilities and prevent security incidents before they occur. An example of reactive security countermeasure is an intrusion detection system that detect security incidents that might be occurring or has already occurred. The authors describe that to have the best protection against security incidents one should implement both proactive and reactive security countermeasures.

1.2. Related work

A study by Demek, Raschke, Janvrin & Dilla [8] indicates that their studied organizations use a reactive social media risk management instead of the recommended proactive social media risk management. To be reactive in social media risk management is described as handling risks ad hoc without a proper information security risk management process done in forehand and reacting to risks as they appear [8].

The OCTAVE Allegro is a proactive risk management method and is described to help organizations go from reactive to proactive, the method is proactive because it recommends doing information security risk management and handle risk proactively before they occur. Di Gangi, Johnston, Worrell & Thompson [14] study showed that organizations social policy mostly focuses on social and legal risks and not so much on the several technical risks that social media may bring. Some of the technical risks social media may bring are for example the risk of getting malware or unauthorized access to social media accounts.

Chi [15] describes that many organizations are unsure of how to develop social media policies so they do not make a social media policy at all or and might prohibit the use of social media instead because of the security concerns. The solution could according to the author be to incorporate the social media policies in the overall information security policies and invest in security tools that cover social media as well. Di Gangi et al. [14] discuss that future research should try to answer if its more effective to incorporate the social media policies in the overall information security policies or keep them separate because of the twofold purpose of social media.

Social media can be used for both personal and professional use and both can affect the organization. Employees using the official organizational social media in an inappropriate way or posting in their own personal social media about the organization can have great effects on organization reputation, like for example two nurses in the UK making jokes about their patients on social media [16]. "*Work life and online life are intertwined, and organizations need to create and communicate policies that help workers understand what behaviors are appropriate*." [4, p. 210].

A review by He [17] showed that organizations were unsure of how to implement an effective social media policy to mitigate social media risks or in other words to be proactive. The results from Demek et al. [8] study indicated organizations use a reactive ad hoc social media policy making instead of being proactive with a thorough recommended risk management process, result do not show how or why this occurs. The authors also imply that the result does not answer to the question if a proactive social media risk management is better than a reactive social media risk management [8]. Comparative studies in the field of social media perceived risks are not really done yet according to Rehman, Baharun & Salleh [18].

The OCTAVE Allegro recommends to be proactive in information security risk assessment [19] but this does not seem to be the case in social media risk management according to [8] [10]. According to Williams & Hausman [10] a lot of research is done in social media risk management but the research mainly focuses on one type of risk like the human/social risk and the social media risk policies are described as reactive by *"…many of the*

recommendations in social media policies are direct responses to social media risks" [10, p. 267].

1.3. Research gap

There is a research gap regarding an answer to how social media risk management is performed and what reasons exists that makes organizations reactive in social media risk management instead of being proactive [8]. There is also a gap in knowledge about if organizations are using a reactive social media risk management process because they are unsure how to implement a proactive social media risk management process [17]. Demek et al. [8] ask for research about if proactive social media risk management is better than a reactive social media risk management.

1.4. Research questions

This study main research question is:
What impact does social media risk management have on organization IT security?

Sub questions to answer the research question:
How is social media risk management performed in Swedish IT organizations?
What are the reasons that social media risk management in IT organizations is reactive or proactive?

1.5. Purpose

The purpose of this study is to investigate and try to describe how social media risk management is performed and what impact social media risk management can have on organizations IT security.

1.6. Delimitation

This study looked at social media risk management and what impact social media risk management had on organizations IT security through prior studies done and through data collected from interviews and surveys. The research was limited to the organization social media, when employees of the organization use (communicate in) the organization social media on the organization owned devices or the employee's own devices.

The delimitation of organizations size in the interviews was 200 up to 8500 employees and in the surveys 15 up to 70 000 employees. The type of organizations that participated was three governmental sector and two private sector in the interviews. And thirteen participates that belonged to the private sector and one participate belonged to the governmental sector in the surveys. The interview and survey participates all worked in IT, in the interviews Social Media experts and IT/Security experts participated. And in the surveys the most common work role of the survey participates was software developer and different types of IT security roles.

2. Literature review

In this section the literature review of the study is presented. First a description of the literature review process then information security is explained and finally social media risks are presented.

2.1. Literature review process

To get relevant literature and to find the key concepts for this thesis Webster & Watson [20] procedure for doing literature review was used. First leading journals was searched through mainly Luleå University of Technology library service EBSCO and Google Scholar.

The found literature was selected on their relevance for the subject of this study and by year. The limitation was made by 10 years (2010) to have a limitation. The relevance was that the literature should be about the IT sector if the content was not very generally made or no other literature was found.

The terms used for search (see Table 1) was: risk, risk management, social media, social media risk, social media risk management, information security risk management, enterprise risk management, IT security, information security, social media risk management model, social media security policy, Web 2.0 security threats, risk treatment, social media policy, proactive reactive security, proactive reactive security countermeasures. The searches were limited to peer reviewed.

Secondly a backward search was done by searching for prior studies in the reference list of the found literature. And lastly a forward search was done in the recommended Web of Science to find literature that cites the previously found literature.

Also, Science Direct service of recommended articles was used when finding relevant literature.

Table 1. Search terms and number of hits in EBSCO

Search term	**Number of hits in EBSCO peer-reviewed and limited to 2010**
“social media risk management model”	1
“social media security policy”	2
“social media risk management”	16
“social media risk”	147
proactive reactive security countermeasures	1018
“social media policy”	1437
web 2.0 security threats	11617
proactive reactive security	16824

2.2. Information Security

Information is an important asset of all organizations, information can represent knowledge, ideas or facts. Information Security is the protection of information systems and the information they contain [21] [22]. The CIA (Confidentiality, Integrity, Availability) triad is used to describe information security and what information security should ensure [12] [21].

The CIA triad is described by Wheeler [12] like:

- Confidentiality is that only authorized parties should be able to access information.
- Integrity is that only authorized parties should be able to change or delete information.
- Availability is about authorized parties should be able to access information the user needs when the user needs it.

To achieve information security, risks to the information assets must be considered. A risk is described by the ISO [11] standard definition like:*" ... the possibility of an effect and, in particular, an effect on objectives"* [11, p. 882]. Risk is described by Jones & Ashenden [23] as the possibility of a threat (person) using a vulnerability to get access to an asset, and to assess risks to an asset, the threat and vulnerability against the value of the asset can be used.

A simple risk assessment can consist of the steps: Identify assets, vulnerability assessment, threat assessment, risk assessment and define countermeasures. After assessment of risks a decision about what to do with the risks should be taken, the four alternatives are described as: avoided, accepted, transferred or mitigated. Avoiding risk is when the assets is not in contact with any vulnerabilities or threats, accepted risk is when the asset risk is at an acceptable level. Transferred risk is when the risk is transferred to someone else to handle, mitigated risk is when the risk is managed to an acceptable level [23].

Risk management is about calculating how much risk the business is willing to cope with against the cost of implementing security controls [12]. Different kinds of famous risk management frameworks are for example (more detailed description in Appendix 3): ISO 31000, ISO/IEC 27005, Octave Allegro and ERM. Controls chosen in a risk management process are used to ensure that the information is confidential, available and to keep the information integrity. These controls can be in the form of for example policies, procedures or hardware to protect information [21].

Choi et al [13] made a quantitative model to give opportunity to calculate the effectivity of proactive and reactive security measures. A given example of proactive security countermeasures is for example a vulnerability management system or a patch management system. The function of proactive security countermeasures is to try to eliminate vulnerabilities and prevent security incidents before they occur. An example of reactive security countermeasure is an intrusion detection system that detect security incidents that might be occurring or has already occurred. The authors describe that to have the best protection against security incidents one should implement both proactive and reactive security countermeasures.

An Information Security Management System (ISMS) can according to ISO [21] be used to manage information security risks and is important for keeping the organization information secure. Procedures, guidelines and policies is used to manage the information security,

various other approaches and controls to improve security. The controls are decided upon in the risk management process, then reviewed, monitored and improved when needed if the risks changes.
Different steps of establishing, monitoring, maintaining and improving an ISMS:

- Identifying information assets and the information security requirements for the assets
- Assess and treat information security risks
- Controls are selected and implemented to manage risks
- Effectiveness of ISMS by controls monitored, maintained and improved [21].

2.3. Social Media Risks

An attempt of categorization of the current business risks of social media is done by Williams & Hausman [10]. Five risk categories and 30 types of risks is found (see Table 2). Four other dimensions was also found, and these dimensions were:

- Evolutionary nature of risk classification is described as risk classification being a continuing work because new risks appear all the time and risk might change its importance over time.
- Risk chains is described as risks affecting each other and can cause chain reactions.
- Risk appetite is described as organizations work in different ways to make their brand known on social media, some in riskier ways than others.
- Risk assessment and risk governance processes is described as the other points classification, risk chains and risk appetite build a base for a risk assessment and risk governance process for social media risks [10].

Di Gangi et al. [14] performed analysis of 40 organizations social media policies and let Delphi panel members identify and prioritize social media risks. Their results were that all panel members found three risks that all panel members agreed on as important was missing in all the studied organizations social media policies. The missing risks in the social media policies but found by panels were; "*unintended exposure of information*", *"damage to consumer confidence"* and *"decreased productivity"* [14, p. 1112].

Table 2. Risk categories and social media risks [10] [14]

Risk Categories and Social Media Risks

Williams & Hausman [10]		**Di Gangi et al** [14]	
Category	**Type**	**Category**	**Type**
Technical	Hacking	**Technical**	Unreliable user-generated content
	Malware		Decreased productivity
	Spam		Uncontrollable actions
	Reliance on external software		Malicious software
	-Availability		Hacks/unauthorized access to social media account
	-Ownership		
	-Continuity		Service interruptions

Human		**Social**	
	Blurring boundaries		
	Psychological harm		Employee views perceived as sanctioned/approved by Employer
	Abusing authority		Online content may be stored or indexed
	Unproductive use of employee's time		Damage to consumer confidence
	Lock out of target group		Unintended exposure of information
	Responsibility		Online content shared with unintended third parties for commercial purposes
	Ethical risks		Inconsistent branding
			Online content shared with unintended third parties for non-commercial purposes
			Inefficient use of employer network resources
			Source of information for hacker/social engineering
			Perception of social media acceptance/adaption
			Minority influence or amplifications of events
			Damage to morale
Compliance	Copyright violations	**Legal**	Intentional or unintentional violation of legal or regulatory requirements
	Violations of laws		Purposeful loss of competitive data or trade secrets
	Identity theft		Social mobilization/online activism
	Audibility		Online content may facilitate discriminatory hiring practices
	Accessibility		
Reputational	Loss of reputation		
	Criticism		
	Language		
	Astroturfing		
	Loss of trust		
Content	Information loss		
	Information overload		
	Loss of intellectual property		
	Disclosure of confidential information		
	Out of date information		
	Loss of information quality		
	Loss of content control		
	Inappropriate/incorrect content		
	Exposure of personal information/loss of privacy		

3. Method

In this section the research strategy for the study is presented and the steps of the study. Then the data collection part is explained and after that follows the data analysis and the ethics of the study. Finally, the validity, reliability, and generalizability of the study is presented.

3.1. Research strategy

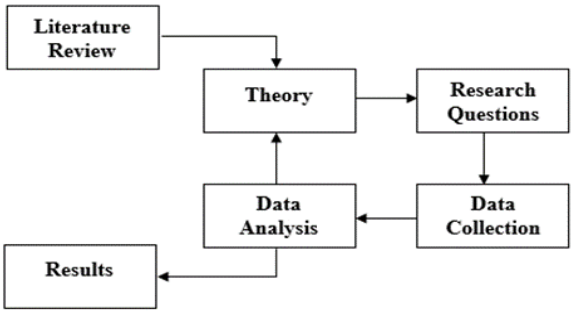

Figure 1. Research steps

The first step in this qualitative study as seen above in (Figure 1) was to perform a literature review to develop the theory part of the study. Then the research questions were formulated and then data collection in form of interviews and surveys was done to try to answer those questions. The data collection and data analysis are described in more detail in following sections.

The purpose of this study was to investigate and try to describe how social media risk management is performed and what impact social media risk management can have on organizations IT security. Therefore, the chosen research strategy for this thesis was qualitative study because of the detailed and extensive description this kind of research gives. Qualitative data collection is when data is collected that is in the form of text and quantitative data is in the form of numbers [24].

This study was first planned to follow the case study research strategy with a multi case study approach to be able to compare different cases of organizations to try to get an answer to the research questions.

In case study a case is investigated in detail and in its own environment [25]. This could not be performed due to not having access to the environment of the interviewees and it was hard to find interviewees. It was hard to find interviewees because many of the organizations did not have employees to handle social media or employees working with social media policy or the organizations responded that they did not have a social media policy. But also, fallout of interviews due to sickness or lack of time from interviewees was experienced.

Other research strategies that was considered [24]:

- Ethnography is a research strategy where the researcher tries to take part in the group it studies to understand the culture. This did not fit as no access was granted into the expert's field.

- Survey strategy gets data from a large group of people for generalization. This could not be used as the number of participants in this study was not large enough.
- Grounded Theory is a strategy for exploration for finding theories grounded in collected field data. This did not fit as no access was granted into the expert's field.
- Design and creation is a strategy where the researcher design and create a new model or artefact. The study did not create any model or artefact, so this was not applicable.
- Action research do something in real world and then reflect on what happened and may repeat it to collect data. Not applicable because this research did not do any action.
- Experiment is a research strategy with the interview person taken into a controlled laboratory environment and asked a set of questions. But this study was seeking to get as detailed answers as possible with the interview person comfortable in their natural environment and it could have been hard to get the interview person comfortable in a controlled laboratory environment [24].

3.2. Data collection

The criteria for selection of candidates in this study were:

- Location: Sweden
- Organization Area: IT
- Role: Employees involved in IT.

The goal of the data collection was to have experts from different fields in IT and from different kinds of organizations. For example, to give the study more width both social media experts and security experts from both private and governmental sectors were included.

Method triangulation is according to Leedy & Ormrod [25] a way to try to validate the results in a qualitative study. Method triangulation is made by using a combination of different data generation methods to get data so that eventual found patterns may be validated by the different methods. First the literature review was done to find the background and form the questions for the qualitative survey and interview. Then to try to triangulate (see Figure 2) the eventual found patterns from the qualitative semi structured interviews and surveys where evaluated against existing data from the literature review.

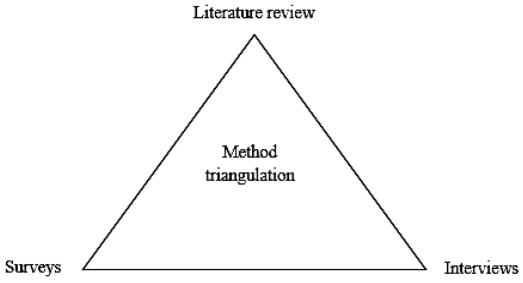

Figure 2. Method triangulation for data collection and data analysis.

The literature review was done to have a ground for building the interview questions and surveys questions. The qualitative interviews and surveys tried to give a bigger description of how social media risk management was performed in different Swedish organizations and

what impact social media risk management could have on an organization's IT security. And to try to show how social media risk management was performed in the organizations and the reasons to the social media policy management being reactive or proactive.

3.2.1. Semi-structured interviews

In this study the interviews was performed in a semi structured manner with 8 starting questions to try to answer how social media risk management is performed in Swedish IT organizations and to give the interviewer a chance to elaborate with more questions if needed to try to get the expert (see Table 3 below) to answer the questions [24].

The interviews were also done to try to answer the question: what are the reasons that social media risk management in IT organizations is reactive or proactive. The interviews were performed in Swedish (see Appendix 2), to try make the interviewed and interviewer more comfortable and to try to minimize misunderstanding due to language barriers. The interview protocol was inspired by the surveys in Demek et al. [8], their results showed that organizations use a reactive social media policy making but not the reasons.

Information about the study and a kind question to participate was posted on personal LinkedIn and Facebook page, four different Facebook groups targeting developers, IT workers and IT security individuals. That gave two interviews. Information about the study and a kind request to participate were also sent to more than 25 organizations by email, in some organizations it was sent to all their local departments in Sweden. In the end it was sent to a lot of email addresses and that gave two interviews. One interviewee emailed and told that a co-worker told about the study and the person wanted to participate in an interview.

Table 3. Interview participates.

		Interview participates				
Participant	**Business Area**	**Organization type**	**Organization size**	**Interview method**	**Duration**	**Date**
Expert 1	Social Media	Governmental sector	900	Telephone	ca 40 min	16/4 2019
Expert 2	Information Security	Private sector	2500	Telephone	ca 15 min	14/5 2019
Expert 3	Social Media	Private Sector	8500	Telephone	Ca 15 min	25/2 2020
Expert 4	Information Security	Governmental sector	800	Telephone	Ca 50 min	1/3 2020
Expert 5	Information Technology	Governmental sector	200	Telephone	Ca 20 min	4/3 2020

3.2.2. Surveys

The survey in this study was done in the free survey tool SurveyMonkey.com. The survey consisted of 10 questions on two pages with an additional line on some questions where extra information could be added. The survey was done to try to answer how social media risk management is performed in Swedish IT organizations. The survey done in Swedish can be seen in (see Appendix 1 Survey) and its original form in English in (Appendix A Supplementary data) from Demek et al. [8].

The response rate was on the low side, the survey and information were posted on personal Facebook and LinkedIn and that gave about four answers. The survey and information were sent to about 50 organizations by email, in some organizations it was sent to all local departments which means the survey was sent to a lot of email addresses and that gave no responses at all.

The method was then changed to posting information and the survey link in four different Facebook groups where the rest of the answers was gathered (see Table 4). The Facebook groups targeted developers, IT workers and IT security individuals.

Table 4. Survey participates.

Survey participates

Survey Participant	Business area	Organization type	Organization size	Work role	Age	Professional experience	Number of certificates	Date of survey
1.	Information Technology Consulting	Private sector	950	Chief Executive Officer (CEO)	49	29	0	25/11 -2019
2.	Grocery	Private sector	15	Technician	31	1	0	1/12 - 2019
3.	Information Technology	Private sector	53	Service Manager	35	7	1	6/12 – 2019
4.	Biotechnology	Private sector	70000	Software developer	35	8	0	6/12 - 2019
5.	Industry Software	Private sector	40	Software developer	36	10	5	5/1 – 2020
6.	Information Technology	Private sector	300	Software developer	37	9	0	5/1 - 2020
7.	Media	Private sector	600	Head of Product	30	10	1	5/1 – 2020
8.	Financial Technology	Private sector	8500	Software developer	27	1	0	5/1 - 2020
9.	Information Technology	Private sector	500	Junior Software developer	38	17	0	5/1 – 2020
10.	Banking and finance	Private Sector	300	Security Engineer	33	1	1	9/2- 2020
11.	Consultant	Governmental sector	-	Cyber Security Specialist	45	20	-	26/2 2020
12.	IT Security	Private sector	3500	Consulting Systems Engineer	40	20	-	26/2 2020
13.	Retail	Private Sector	4000	Information Security Manager	50	30	1	27/2 2020
14.	Bank	Private Sector	15714	Information Steward	45	21	-	27/2 2020

3.3. Data analysis

Thematic analysis is when the researcher tries to analyse and find themes in the collected data. Theoretical thematical analysis is deductive and is when data is analysed after already found themes by other researchers. Inductive thematical analysis is when data is analysed without any previous research to compare with [26] .

In this study the data analysis of the surveys and interviews was theoretical thematical, that means that already existing risk themes found by Williams & Hausman [10] and Gangi et al [14] was used for analysis to have a pattern to start analysing the interview and survey data.

The analysis started to try to see if the existing risks themes are present in the Swedish organizations in the study. (To see full themes for risk categories, see Table 2).

Table 5. Themes for analysis or risks present in Swedish organizations in the study

Themes for analysis of risk present in organizations in the study	
Risk categories inspired by Williams & Hausman [10]	**Risk categories inspired by Gangi et al [14]**
– Technical – Human – Content – Compliance – Reputational	– Social – Technical – Legal

The risk themes above (see Table 5) mends together like technical goes with technical, human with social and compliance with legal.

Risk categories explanation [10]**:**

- **Technical** social media risks caused by not having social media risk management be for example hacking of the social media account to gain access to information (content), malware that can occur in social media applications to harm organization systems.
- **Human/Social** media risks can consist of it being difficult to separating private social media from organization social media. This can cause a confusion about responsibility in the use of social media in organization name. But also, ethical risks exist that can make employees involve in improper behaviour or breach confidentiality of the organization's information.
- **Content social** media risks can be loss of information because of employee disclosure or short messages in social media can cause information quality loss for example.
- **Compliance/Legal** social media risks can be employees violating laws or sharing content with copyright.
- **Reputational** social media risks can someone posting misleading in social media as the organization and that can cause loss of reputation or loss of trust by employees/customers [10].

The interview notes were analysed to find risks by already existing themes. The analysis started to try to see if the existing risks are present in the Swedish organizations in the study. In the interview notes five quotes (see Table 6) was found that could be considered to suit the risks themes.

Table 6. Risk Category themes for analysis of risks

	Interviewee quotes that matched risk themes				
Expert / **Risk Theme**	**Expert 1:**	**Expert 3:**	**Expert 3:**	**Expert 5:**	**Expert 4:**
	"There is no risk management plan in place to identify or handle risks associated with social media right now"	"Social media is used for communication by employees in some parts of the organization but not in the whole organization."	"You are supposed to use common sense regarding social media. Different departments can have different rules but there are no general regulations for the use of social media on the workplace."	"It should not be monitored all the time, that would indicate something is wrong. You should be able to trust your employees."	"There is a lot to protect against. Things needs to be updated, patched and people educated, so the risks with social media is not really prioritized."
Technical	X	X	X		X
Human/Social	X	X	X	X	X
Content	X	X	X		X
Compliance/Legal	X	X	X	X	X
Reputational	X	X	X		X

In this study the interviews and survey analysis were done to try to answer the research questions:

- What impact does social media risk management have on organization IT security?
- How is social media risk management performed in Swedish IT organizations?
- What are the reasons that social media risk management in IT organizations is reactive or proactive?

3.4. Ethics

The interview persons were contacted by mail, Facebook/Facebook messenger or on LinkedIn and the interviews was done on telephone. As recommended by Leedy & Ormrod [25] I did the notes by hand as the interview went on, and later mailed/messaged the interviewees and got their consent on the interview transcript so that the interviews were interpreted right. The interviewees were also told they can be anonymous and some of the participants wished to be anonymous. Therefore, the participants are called by numbers instead of by name.

3.5. Validity, reliability, and generalizability

The quality of qualitative studies can be reviewed with the term's validity, reliability and generalizability. The validity is how suitable the way to collect data is, if the research questions and method to get data is suitable but also if the way to analyse data gives valid data to the degree that is expected [27].

The validity in this study was worked on by using method triangulation [25]. The literature review was done to form the research questions, the background, the questions in the survey and interviews. The literature review, the interview data and the survey data were then used to try to triangulate the study results.

To give the data for the study some width both private and governmental sector organizations and experts from both security and social media was interviewed. The way to analyse data was with a theoretical thematical method to try to see if already found risk themes could be found in the collected data [26].

Reliability is if the study can be replicated with the same process and get similar results [28]. The research method was described by steps taken in the research strategy, the interview and survey protocols were added in the appendix. Data collection and data analysis was also described so that it is possible to replicate the study if wanted.

Generalizability is if the results from the study sample can be used for a bigger population than the study sample [27]. This studies interview and survey sample aim was not to generalize but should give some insight in how social media risk management was performed in Sweden. But it was hard to say that the result is generalizable to other bigger populations without knowing the results of a bigger study.

4. Results - Analysis of semi structured interviews and surveys

In this section the results of the analysis are presented. First the analysis of the results from the semi-structured interviews. Then follows a description of the social media risk management in five organizations in Sweden. After that follows, an analysis of the result from the surveys. The risks found in the survey organizations and then lastly social media risk management in the survey organizations.

The risks found in the interviews and surveys was used to find what risks were present in the partaking organizations. The social media risk management section in both interviews and surveys were used to try to give a description of how social media risk management was handled in Swedish organizations. The analysis was done to try to answer the studies research questions.

The interviews had five participants that consisted of three interviewees that belonged to the governmental sector and two interviewees that belonged to the private sector.

4.1. Social Media Risk Management in interviewed organizations

Figure 3. Expert Interview Results

In the chart above (Figure 3) the results from the interviews with five experts are presented. This study can hopefully give an insight to how social media risk management was handled in Sweden.

In the case of risk management plan, the experts told they had some kind of risk management plan in three out of five interviewed organizations. But this was in two of the cases described as a more general risk management. Two of those organizations were private and one was governmental. The both experts who told they did not have a risk management plan particularly for social media belonged to governmental organizations.

Three out of five interviewed experts told they had a social media policy. Two of those organizations was governmental and one was private. Two organizations did not have a social media policy, one governmental and one private.

In the case of monitoring social media in the organization, three out of five experts told that their organizations did monitoring of social media. Two of those organizations was governmental and one private. One private organization expert told they only monitored social media on indication and one private organization did not monitor social media at all.

Audits on social media was done by two of five organizations. One private organization and one governmental. Two governmental organizations experts told they only did social media audits on indication and one private organization did not do audits on social media at all.

The experts told they handled their social media risk management by being reactive in three out of five organizations. All three of those reactive organizations was governmental. The two experts who told they were proactive in social media risk management belonged to private organizations.

4.2. Reactive Risk Management for Social Media in interviewed organizations

Social media risk management in this study was reactive in three out of five organizations, all three were governmental organizations. Expert 1 in a governmental organization described they did not have any risk management plan for social media, but they were working on both guidelines and policies for social media. Risk awareness existed but not in document form and risk management analysis was done but only verbally and not written down.

Social media was monitored by the organization by channel responsible that had moderating responsibility. Social media was also audited by moderating. The organization was described as more reactive but also proactive to a certain degree. They described they could be more proactive by thinking more distinctly and systematically about what information is communicated in their channels (both traditional channels and internal/external social media).

An expert in a governmental organization described there are so many risks to protect against that there is not enough time to prioritize social media. **Expert 4**:" *We are reactive. There is not enough time to be proactive against everything. There is a lot to protect against. Things needs to be updated, patched and people educated, so the risks with social media is not really prioritized.".*

There were policies for the use of social media on the workplace, but no risk management plan existed. A general external environment monitoring that was updated through CERT.se existed. To be more proactive they could have more user education and formulate a more distinct framework for social media.

Another expert in a governmental organization told that they are reactive in the terms of cyber security, mainly because of older systems. They wanted to be proactive, but in the end problems are handled as they appear. The organization was proactive with softer values like how the employees are hired and employees got education in what they were allowed to do and not. **Expert 5:** "*Social media is audited by security level and on indication. Personal social media is also audited in the hiring process."*

4.3. Proactive Risk Management for Social Media in interviewed organizations

The experts who told their organizations are proactive was both in private sector organizations.

An expert in a private organization told they are proactive and in the case of being proactive they were doing what was possible. They had a general information security policy and separate policies for social media. Also, a policy for the use of social media on the workplace existed. **Expert 2:** "*Social media is monitored by the organization by the publisher. Some employees can post in social media and these posts are reviewed against the policy."*

An expert in another private organization described they were proactive and there existed risk management plans and policies for basically everything. The risk management plans and policies were described as both enough and not, there was always holes to fill. **Expert 3: "***You are supposed to use common sense regarding social media. Different departments can have different rules but there are no general regulations for the use of social media on the workplace."* The expert described the organization always questioned about what impact things could have for their customers and staff and had a great respect for data and security.

4.4. Results from surveys

In this section the analysis of the surveys in the study are presented. The survey had fourteen participants that consisted of thirteen participates that belonged to the private sector and one participate that belonged to the governmental sector.

Professional experience ranged from 1 year up to 30 years of experience. The business areas varied a lot, but the most common work role of the survey was software developer and different types of IT security roles. The smallest organization in the survey was an organization consisting of 15 employees and the largest organization consisted of 70 000 employees.

4.5. Social media risks in organizations survey participants

- **Human/Social risk**

Survey participants was asked if the organization is concerned (see Figure 4) about if the employees personal use of social media at work negatively impacts productivity. 11 out of 14 participants did not think their organization was concerned about that risk. This **human/social risk** was not a concern according to the survey participants.

- **Compliance/Legal risk**

Next question was if the organization is concerned about litigation due to social media use and 7 participants answered that they neither agree or disagree and the other 7 disagrees or strongly disagree. This **compliance/legal risk** was not a concern for the organizations.

- **Content risk**

The question if the organization is concerned about intellectual property leakage due to social media use five participants answered agree or strongly agree. Four participants strongly disagree or disagrees. Five participants answered that they neither agree or disagree. There was a slight concern about the **content** risk in the survey organizations.

- **Technical risk**

The question if the organization are concerned about that viruses and malware could be introduced into organization network because of employee use of social media. Six participants strongly agreed or agreed. Five participants answered that they neither agree or disagree. This **technical** risk was a concern in the organizations in the survey.

- **Reputational risk**

The questions if the organization is concerned about that their product/services will be portrayed in a negative light by consumer using social media seven disagreed or strongly disagreed. Five participates either agree or strongly agree. This **reputational** risk did not seem to be a risk in the organizations.

The last question about concern is if the organization is concerned about the use of social media can damage their reputation. Seven participants answered strongly disagree or disagree. Five participants either agree or strongly agree. This **reputational** risk did not seem to be a risk in the organizations.

Figure 4. Organization concerns

4.6. Social Media Risk Management in survey organizations

The question if the organization had a risk management plan for identifying and managing risks with social media eight survey participates answered no and six answered yes. The question about if the organization had an established policy on social media use in the workplace nine participates answered yes and five participates answered no.

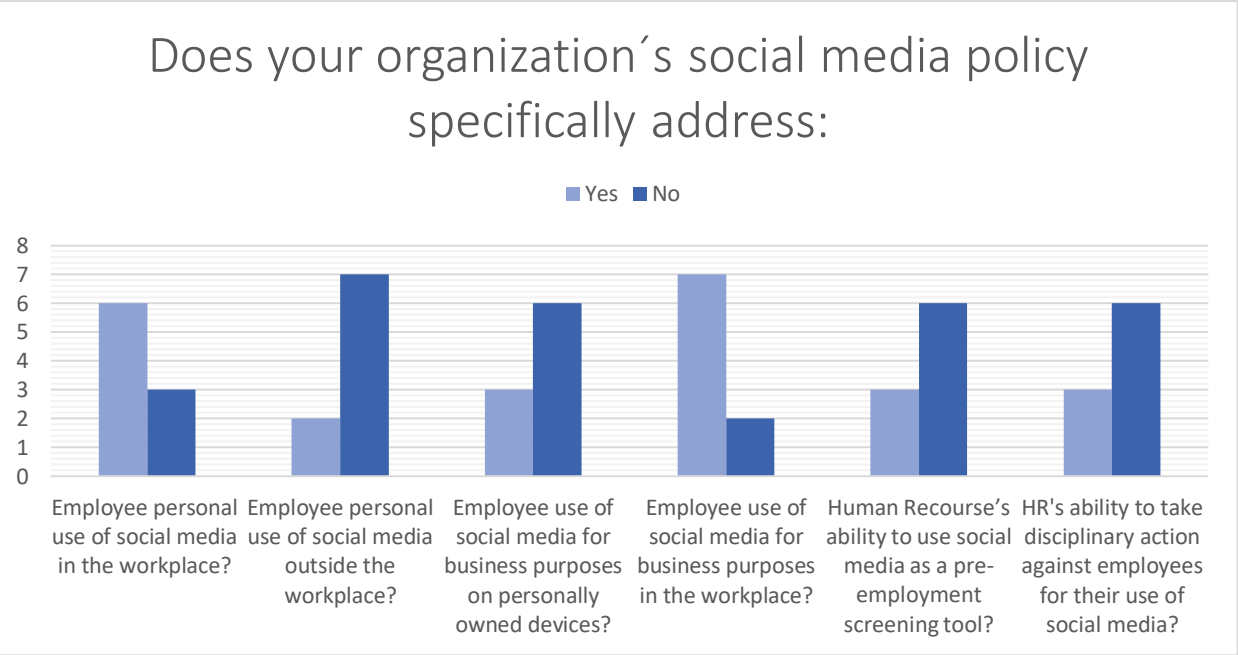

Figure 5. Does your organization´s social media policy specifically address

In the cases where there existed a social media policy the participates (see Figure 5) was asked if the policy included personal use of social media at the workplace six out of nine participates answered yes and three answered no. The question if the social media policy includes personal use of social media outside of the workplace seven out of nine answered no and two answered yes.

Next question was if the organization social media policy specifically addresses employee use of social media for business purposes on personally owned devices. Six answered no and three answered yes. The question if the organization social media policy specifically addresses employee use of social media for business purposes in the workplace seven answered yes and two answered no.

If the organizations social media policy specifically addresses human resources ability to use social media as a pre employment screening tool six out of nine participants answered no and three answered yes. The last question regarding if the social media policy specifically addresses human resources ability to take disciplinary action against employees for their use of social media, six out of nine participates answered no and three answered yes.

If the organization has adequate technical controls (see Figure 6) to support social media policies nine out of fourteen participants answered that they neither agree or disagree. Two strongly agree and one agree. One participant disagrees and one strongly disagrees. The question if organizations have adequate training in place for employees to ensure they

understand appropriate use of social media six out of fourteen participants neither agree or disagree. Four participants agree and three strongly agree. One participant disagrees.

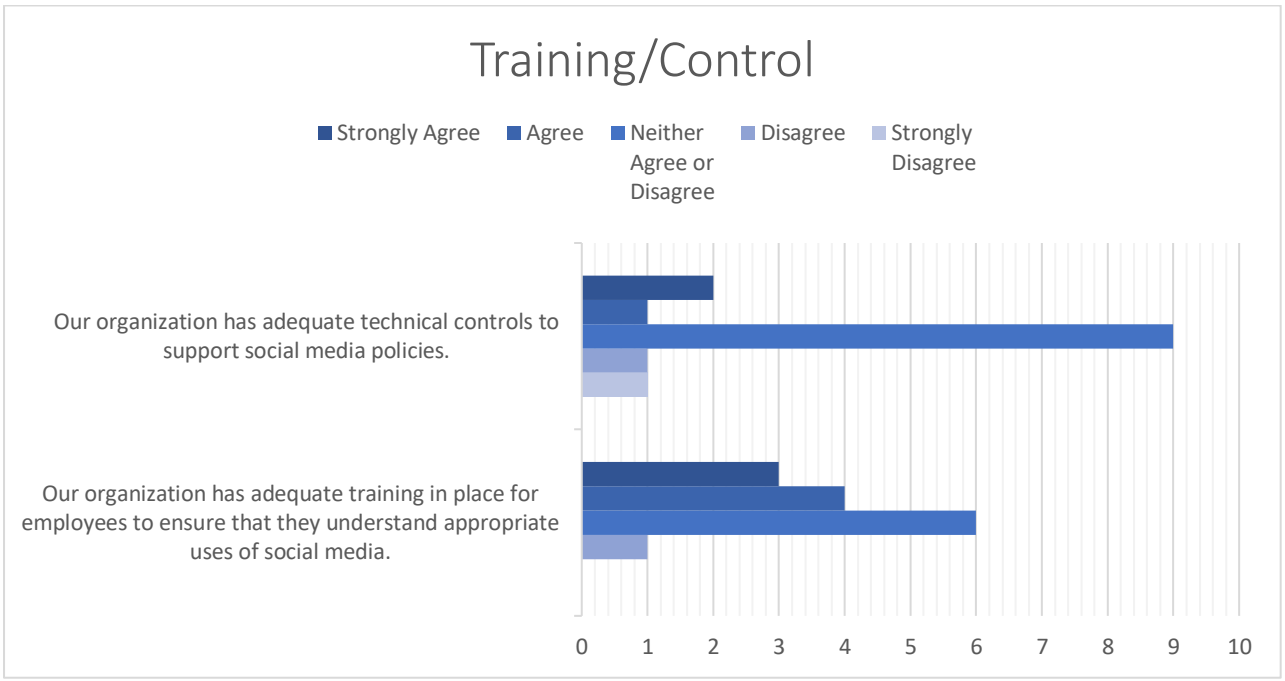

Figure 6. Training/Control

The question if the organization regularly audit social media use got ten no and four yes answers. If the organization regularly monitor the social media got eight no and six yes answers.

5. Discussion

In this section the discussion is presented. First the discussion of the research questions is presented, then follows the discussion of the research method.

5.1. Discussion of the research questions

The research gap that formed this study was how social media risk management is performed and what reasons exists that makes organizations reactive in social media risk management instead of being proactive [8]. There was also a gap in knowledge about if companies are using a reactive social media risk management process because they are unsure how to implement a proactive social media risk management process [17].

5.1.1. How is social media risk management performed in Swedish IT organizations?

Social risk management was according to this study performed mostly reactive and most of the organizations did not perform risk management specifically for social media. More organizations had a social media policy than performed risk management for social media. Which implies the organizations create a social media policy without performing the risk management process.

The experts in this study expressed that they knew risk management is important but three out of five organizations in the interviews and eight out of fourteen organizations in the surveys did not have any risk management specifically for social media. There was some reasons told in the interviews, as that there is not enough time to handle all risks, the systems are so old that it was hard to be proactive or work is currently done to be able to perform social media risk management.

Three out of five experts who described themselves as reactive was governmental. The two experts who described themselves as proactive in social media risk management belongs to private organizations.

The two private organizations told they had general security policies, risk management plans for basically everything and described themselves as proactive. But one of the experts who described themselves as proactive did not have a social media policy. **Expert 3: "***You are supposed to use common sense regarding social media. Different departments can have different rules but there are no general regulations for the use of social media on the workplace."*. Using common sense as a proactive social media risk management seems very risky as common sense may not the same for every employee. A better description of the organization would be that they are proactive in their overall risk management but reactive in social media risk management.

5.1.2. What are the reasons that social media risk management in IT organizations is reactive or proactive?

The results from Demek et al. [8] study indicated organizations use a reactive ad hoc social media policy making instead of being proactive with a thorough recommended risk management process, their result do not show how or why this occurs.

The risk management for social media in the IT organizations in this study was described in interviews as reactive due to several reasons. Old systems that made it hard to be proactive,

lack of time for prioritizing social media risks or risk management was currently being worked on. One expert also described they strive to be proactive but in the end things are handled when they occur.

The proactive IT organizations described themselves as having a general security policy and risk management plans for basically everything. One expert described their risk management plans and policies as both enough and not, more can always be done.

The gap of knowledge in that organizations are using a reactive risk management because they are unsure how to implement proactive social media risk management was not true in this study. The interviewed organizations all knew how to be proactive but for some different reasons stopped them from being it.

Three out of five organizations in the interviews and nine out of fourteen survey organizations had a policy for social media. But only two out of five organizations in the interviews and six out of fourteen organization in the survey did risk management specifically for social media. So, this confirms Demek et al. [8] research that some organizations do a social media policy without doing a risk management process for social media.

The recommended way by several information security risk management frameworks [11] [19] [29] [30] [31] is to do the risk management process first and then implement policies to counter the found risks and be proactive. Creating policies without a risk management process generates that a lot of risks may be missed.

The interviews also revealed that training and educating employees helped with the technical risks of social media, this was also described by Di Gangi et al. [14] Delphi panel results. The research gap regarding if proactive social media risk management is better than reactive did not get an answer in this study. Previous research describe that the best social media risk management is done both proactive and reactive [13].

5.1.3. What impact does social media risk management have on organization IT security?

Social media risks can lead to risks that impacts organization IT security. In the interview notes five quotes was found that could be considered to suit the risks themes.
It was hard to point out clearly what risks suited the quotes because they all affect each other in some way. That they affect each other is also pointed out by Williams & Hausman [10, p. 271]: *"Some risks are direct consequences of the capabilities of the technology or of the behavior and actions of people…"*

Risks themes: Technical, Human/Social, Content, Compliance/Legal & Reputational

Expert 1: *"There is no risk management plan in place to identify or handle risks associated with social media right now".*

Expert 3: *"You are supposed to use common sense regarding social media. Different departments can have different rules but there are no general regulations for the use of social media on the workplace."*

Expert 4: *"There is a lot to protect against. Things needs to be updated, patched and people educated, so the risks with social media is not really prioritized."*
Risk management is done to calculate how much risk the business is willing to handle [12]. The controls chosen in the risk management process can be in the form of policies, procedures or protective hardware and the controls are chosen to ensure confidentiality, availability and integrity of the organization information [21].

Different kinds of famous risk management frameworks are for example (more detailed description in Appendix 3): ISO 31000, ISO/IEC 27005, Octave Allegro and ERM. Not having risk management or regulations for social media can cause social media risks like technical, human/social, content, compliance/legal and reputational risks [10].

A social media policy should be in place to guide employees about appropriate behaviour on social media [4]. The risk with employing common sense regarding social media regulation is because what you consider as common sense might be something completely different for someone else. If an employee performed something incorrect, that would make it hard to implement repercussions if no regulations exists but common sense. The employee might also feel unsecure about the "rules" changing if no regulations exist.

The risk with not prioritizing social media can cause all the above risks but in the end the social media risk might also be unprioritized because of worse consequences occurring if it is prioritized over other risks.

Risks themes: Technical, Human/Social, Content, Compliance/Legal & Reputational

Expert 3: *"Social media is used for communication by employees in some parts of the organization but not in the whole organization."*

Social media applications can be unsecure and confidentiality of the organization information that is shared on social media can be at risk of exposure [32]. The risks of shared organization information on social media can be technical, human/social, content, compliance/legal and reputational**.**

Risks themes: Human/Social & Compliance/Legal Risks

Expert 5:*" It should not be monitored all the time, that would indicate something is wrong. You should be able to trust your employees."*

Trust is a complicated issue to depend on in information security. Humans make mistakes and having regulations help employees know what behaviour is right or wrong. Not monitoring and archiving the social media activities of employees can cause human/social and compliance/legal risk. Education and monitoring social media activities with the use of technology may enforce the social media policy and may stop employees from uploading sensitive information upon social media applications [17] [33].

5.2. Method discussion

Regarding the method of the study, case study was first the chosen research method for the study but had to be discarded due to not getting access to the interviewee's environments. The qualitative research method was then chosen and fitted the study because the study was aiming to answer a question of how organizations social media risk management is performed, and the reasons to the social media risk management in IT organizations being reactive or proactive. The study aimed to answer the above questions to hopefully be able to describe how social media risk management is performed and what impact it can have on organization IT security.

A lot of time was put on the literature review and in retrospect more time should have been put into searching for interviewees and survey participants. It was hard to get participants to interview and to perform the survey. The method of getting interviewees and survey participants was per email, on Facebook and LinkedIn. This method was not that successful because the response rate was sparse but finding more participants in the time limit was not possible. Many companies seemed reluctant to talk about security with a stranger on email and that is fully understandable. Maybe more personal contacts could have been used to try to get more interviews, but it was hard getting any responses at all. The method of performing the interviews was by telephone and the interviewer may possibly have affected the interviewee by tone of voice or leading questions, but this was countered as good as possible by trying to be neutral. The telephone interviews were a positive experience and it was very interesting to hear how different organizations work with their social media risk management.

Some organizations responded they did not perform social media risk management and did not suit the study even if stated that all organizations were welcome to participate. One organization responded by email that they did not perform social media risk management but gave contact information to their information security department. When in telephone interview with the information security responsible, the person told that their role included social media risk management and they do in fact perform social media risk management. So, confusion about if social media risk management was done seems to exist and some possible interviewees might have disappeared due to not knowing what the information security department works with.

6. Conclusion

The purpose of this study was to investigate and try to describe how social media risk management is performed and what impact social media risk management could have on organizations IT security.

Generalization of the result was not an aim with this study because of the number of participants in the study but the results could hopefully be a contribution to both research and practitioners of how some Swedish IT organizations handled their social media risk management and what risks this could cause to the organization's IT security.

This research is important because it was requested by previous researchers as seen in (1.1 Background) and (1.2 Problem Statement). The research was done with the research method qualitative study with qualitative interviews to get more deeply going answers and by surveys to get data to compare the interviews with.

The outcome of this study was possible knowledge for researchers and for practitioners in the field, of how social media risk management was handled in some organizations in Sweden and what impact the chosen form of social media risk management could have on the IT security.

Five semi structured interviews and fourteen surveys was performed to try to answer the research questions that were:

6.1. How is social media risk management performed in Swedish IT organizations?

The majority of the experts described their organizations as reactive and to not have risk management specifically for social media. More organizations have a social media policy than perform risk management for social media.

So, this confirmed Demek et al. [8] research that some organizations do a social media policy without doing a risk management process for social media.

6.2. What are the reasons that social media risk management in IT organizations is reactive or proactive?

The experts described their social media risk management in interviews as reactive due to several reasons: old systems that made it hard to be proactive, lack of time for prioritizing social media risks or risk management for social media is currently being worked on.

The experts described their proactive IT organizations as having a general security policy and risk management plans for basically everything.

6.3. What impact does social media risk management have on organization IT security?

Social media risks can lead to risks that impacts organization IT security. In the interview notes five quotes was found that could be considered to suit the risks themes:
Expert 1: *"There is no risk management plan in place to identify or handle risks associated with social media right now".*

Expert 3: *"You are supposed to use common sense regarding social media. Different departments can have different rules but there are no general regulations for the use of social media on the workplace."*
Expert 4: *"There is a lot to protect against. Things needs to be updated, patched and people educated, so the risks with social media is not really prioritized."*
Not having risk management or regulations for social media can cause social media risks like technical, human/social, content, compliance/legal and reputational risks [10].

Expert 3: *"Social media is used for communication by employees in some parts of the organization but not in the whole organization."*
The risks of shared organization information on social media can be technical, human/social, content, compliance/legal and reputational**.**

Expert 5:*" It should not be monitored all the time, that would indicate something is wrong. You should be able to trust your employees."*.
Trust is a complicated issue to depend on in information security. Humans make mistakes and having regulations help employees know what behaviour is right or wrong. Not monitoring and archiving social media activities of employees can cause human/social and compliance/legal risk.

6.4. Future research/Limitations

This research topic was very interesting, and one could go in a lot of different ways in researching it. Future research could try to get a bigger response rate in the interviews and surveys and see if it changes the results. Also, to compare the social media policies in Sweden would have been interesting to see if they differ from existing results of studies of social media policies. This study only got access to one organization social media policy and it would have been interesting to see other organizations social media policies.

The research gap if proactive social media risk management is better than reactive did not get an answer in this study so that would also be an interesting research to continue with. One more interesting thing to research would be to ask organizations what would make them more willing to prioritize social media risks. Are the social media risks consequences too small to make social media risk management prioritized before something occurs or should it be included in the overall information security risk management as suggested by Chi [15]

References

[1] N. B. Ellison and D. M. Boyd, “Sociality Through Social Network Sites,” *The Oxford Handbook of Internet Studies,* 2013.

[2] M. Cross, “Social Media Security : Leveraging Social Networking While Mitigating Risk,” 2014. [Online]. Available: https://doi-org.proxy.lib.ltu.se/10.1016/C2011-0-09032-4. [Accessed 30 November 2018].

[3] N. G. Barnes, M. D. T. Tran, N. Khalil, S. Pavao and K. Maloney, “The 2017 Inc. 500 & Social Media: Finding Its Place in the Marketing Mix,” University of Massachusetts Dartmouth, Massachusetts, 2018.

[4] K. W. O’Connor, G. B. Schmidt and M. Drouin, “Helping workers understand and follow social media policies,” *Business Horizons,* vol. 59, no. 2, pp. 205-211, 2016.

[5] N. R. Shah and S. K. Jha, “Exploring Organisational Understanding of Foundational Pillars of Social Media - A Qualitative Content Analysis of Social Media Policies of Technology Companies,” *Journal of Management Research,* vol. 18, no. 4, pp. 226-245, 2018.

[6] S. S. Gupta, A. Thakral and T. Choudhury, “Social Media Security Analysis of Threats and Security Measures,” in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE),* Paris, 2018.

[7] C. Oehri and S. Teufel, “Social media security culture,” in *2012 Information Security for South Africa,* Johannesburg, 2012.

[8] K. C. Demek, R. L. Raschke, D. J. Janvrin and W. N. Dilla, “Do organizations use a formalized risk management process to address social media risk?,” *International Journal of Accounting Information Systems,* vol. 28, pp. 31-44, 2018.

[9] D. Haynes, “Social media, risk and information governance,” *Business Information Review,* vol. 33, no. 2, p. 90–93, 2016.

[10] S. P. Williams and V. Hausman, “Categorizing the Business Risks of Social Media,” in *CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies*, Barcelona, 2017.

[11] G. Purdy, “ISO 31000:2009 - Setting a New Standard,” *Risk Analysis - An International Journal,* vol. 30, no. 6, pp. 881-886, 2010.

[12] E. Wheeler, “Security Risk Management - Building an Information Security Risk Management Program from the Ground Up,” 2011. [Online]. Available: http://eds.b.ebscohost.com.proxy.lib.ltu.se/eds/ebookviewer/ebook/bmxlYmtfXzM2NTU1M19fQU41?sid=692376b7-3d69-4520-9b41-359ecba3ca50@pdc-v-sessmgr06&vid=3&format=EB&rid=1. [Accessed 23 november 2018].

[13] Y.-H. Choi, H.-Y. Jeong and S.-W. Seo, “A quantitative model for evaluating the efficiency of proactive and reactive security countermeasures,” *IEICE Transactions on Information and Systems,* pp. 637-648, 1 march 2015.

[14] P. M. Di Gangi, A. C. Johnston, J. L. Worrell and S. C. Thompson, “What could possibly go wrong? A multi-panel Delphi study of organizational social media risk,” *Information Systems Frontiers,* vol. 20, no. 5, p. 1097–1116, 2018.

[15] M. Chi, “sans.org,” 16 march 2011. [Online]. Available: https://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749. [Accessed 10 march 2018].

[16] R. Hill, “NHS smacks down hundreds of staffers for dodgy use of social media, messaging apps,” *theregister,* 17 september 2018.

[17] W. He, “A review of social media security risks and mitigation techniques,” *Journal of Systems and Information Technology,* vol. 14, no. 2, pp. 171-180, 2012.

[18] Z. U. Rehman, R. Baharun and N. Z. M. Salleh, “Antecedents, consequences, and reducers of perceived risk in social media: A systematic literature review and directions for further research,” *Psychology of Marketing,* vol. 37, no. 1, pp. 74-86, 2020.

[19] R. A. Caralli, J. F. Stevens, L. R. Young and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," 2007. [Online]. Available: https://ltu.instructure.com/files/818847/download?download_frd=1. [Accessed 30 November 2018].

[20] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. 26, no. 2, pp. xiii-xxiii, 2002.

[21] The International Organization for Standardization (ISO), "ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary," february 2018. [Online]. Available: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip. [Accessed 18 february 2019].

[22] M. Nieles, K. Dempsey and V. Y. Pillitteri, "An Introduction to Information Security," 2017. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-12r1. [Accessed 25 november 2018].

[23] A. Jones and D. Ashenden, "Risk Management for Computer Security : Protecting Your Network and Information Assets," Oxford, Elsevier, 2005.

[24] B. J. Oates, Researching Information Systems and Computing, London: Sage Publications Ltd, 2013.

[25] P. D. Leedy and J. E. Ormrod, "Practical Research Planning and Design," 2014. [Online]. Available: https://libris-kb-se.proxy.lib.ltu.se/bib/14855095. [Accessed feb 2020].

[26] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006.

[27] L. Leung, "Validity, reliability, and generalizability in qualitative research," *Journal of Family Medicine and Primary Care*, vol. 4, no. 3, pp. 324-327, 2015.

[28] A. K. Morgan and V. B. Drury, "Legitimising the subjectivity of human reality through qualitative research method," *The Qualitative Report*, vol. 8, no. 1, pp. 70-80, 2003.

[29] The International Organization for Standardization (ISO), "ISO 31000 - Risk management," February 2018. [Online]. Available: https://www.iso.org/publication/PUB100426.html. [Accessed 15 february 2019].

[30] T. I. O. o. S. (ISO/IEC), "International Standard - ISO/IEC 27005:2008 - Information Technology- Security techniques - Information Security Risk Management," 15 june 2008. [Online]. Available: https://www.sis.se/api/document/preview/909897/. [Accessed 13 february 2019].

[31] The Committee of Sponsoring Organizations (COSO), "https://www.coso.org/Pages/erm.aspx," 2019. [Online]. Available: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf. [Accessed 23 january 2019].

[32] S. Kumar and S. K. Deepa, "On Privacy and Security in Social Media – A Comprehensive Study," in *International Conference on Information Security & Privacy (ICISP2015)*, Nagpur, 2015.

[33] D. Tayouri, "The human factor in the social media security –combining education and technology to reduce social engineering risks and damages," in *6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015*, Israel, 2015.

[34] S. Halliday, K. t. Badenhors and R. von Solms, "A business approach to effective information technology risk analysis and management," *Information Management & Computer Security*, vol. 4, no. 1, pp. 19-31, 1996.

[35] C. Preimesberger, "How Enterprises Can Better Defend Against Social Media Threats.," *eWeek*, pp. 2-3, 24 september 2018.

[36] R. Alguliyev, R. Aliguliyev and F. Yusifov, "Role of Social Networks in E-government: Risks and Security Threats," *Online Journal of Communication and Media Technologies*, vol. 8, no. 4, pp. 363-376, 2018.

2 Appendix

Appendix 1 Survey

Inspired from [8] survey in Appendix A. Supplementary data from *"Do organizations use a formalized risk management process to address social media risk?"*.

Personligt

Arbetstitel: _____

Antal certifieringar: _____

Ålder: _____

Arbetserfarenhet i år totalt: _____

Arbetsgivare

Är organisationen: Statlig ☐ Privat ☐

Industri: _____

Antal anställda: _____

Sociala media kan användas av människor för att utbyta information eller innehåll, samarbeta och för en hel del mer. Exempelvis vanliga media som nyheter på en TV ger inget utbyte mellan människor medan sociala medier låter användare kommentera, diskutera och dela nyheter. Frågorna nedan ska ses i sammanhang av din organisations användande och riskhanteringspraxis kring sociala media.

Vilka typer av sociala media tillämpas av din organisation:	**Tillämpas nu**	**Finns planer på tillämpning**
Sociala nätverk (t.ex. Facebook)		
Bloggar (t.ex. Wordpress)		
Mikrobloggar (t.ex. Twitter och Tumblr)		
Bild och video delande nätverk (t.ex. Youtube och Flickr)		
Positions baserade recensions nätverk (Foursquare och Yelp)		
Professionella nätverk (t.ex. LinkedIn)		
Social bokmärkning (t.ex. Pinterest)		
Annan:		

Malena Holmstedt
holmal-4

	Instämmer inte alls	**Instämmer inte**	**Varken instämmer eller instämmer inte**	**Instämmer**	**Instämmer helt**
Organisationen är oroad över att användandet av sociala medier kan skada vårat rykte.					
Organisationen är oroad över att våra produkter/tjänster kommer framställas negativt av kunder/användare på sociala medier.					
Organisationen är oroad att virus och malware kan spridas i organisationens nätverk av anställda som använder sociala medier.					
Organisationen är oroad över att intellektuell egendom kan läcka ut på grund av användandet av sociala medier.					
Organisationen är oroad över rättstvist på grund av sociala medier.					
Organisationen är oroad att anställdas privata användande av sociala medier påverkas produktiviteten på arbetet.					

Organisationen använder:	**Instämmer inte alls**	**Instämmer inte**	**Varken instämmer eller instämmer inte**	**Instämmer**	**Instämmer helt**
Sociala medier för att förbättra kommunikationen med kunder/användare.					
Sociala medier för att skapa kundintresse eller försäljning.					
Sociala medier för att förbättra och underhålla vårat varumärke.					
Sociala medier för att utveckla nya produkter/tjänster.					

Malena Holmstedt
holmal-4

Sociala medier för att rekrytera ny personal.					
Sociala medier för att kommunicera med anställda.					

Har din organisation en riskhanteringsplan för att identifiera och hantera risker som finns med användandet av sociala medier?

Ja___ Nej___ Om Ja, vem är ansvarig för programmet (rollen)?_____

Har din organisation en etablerad policy över användandet av sociala medier på arbetsplatsen?

Ja___ Nej___

Om Ja, nämner organisationens policy specifikt följande:	**Ja**	**Nej**	**Kommentarer**
Anställdas privata användande av sociala medier på arbetsplatsen?			
Anställdas privata användande av sociala medier utanför arbetsplatsen?			
Anställdas användande av sociala medier för organisationens ändamål på privat ägda enheter?			
Anställdas användande av sociala medier för organisationens ändamål på arbetsplatsen?			
Human Resources (HR) användande av sociala medier för utgallring av arbetssökande?			
HR´s möjlighet till disciplinära åtgärder mot anställda för deras användande av sociala medier?			

	Instämmer inte alls	**Instämmer inte**	**Varken instämmer eller instämmer inte**	**Instämmer**	**Instämmer helt**
Organisationen har tillräcklig utbildning för att anställda ska kunna förstå vad som är passande användande av sociala medier.					
Organisationen har tillräcklig med teknisk kontroll för att upprätthålla sociala medier policys					

Övervakas sociala medier regelbundet av organisationen? Ja ____ Nej ____

Om Ja, vilken avdelning sköter detta? _____

Granskas användandet av sociala medier rutinmässigt av organisationen? Ja ____ Nej ____

Om Ja, vem gör granskandet (rollen)?_____

Tack för att du ville delta i enkäten! Din feedback är viktig

Malena Holmstedt
holmal-4

Appendix 2 Interview

Inspired from [8] survey in Appendix A. Supplementary data from "Do organizations use a formalized risk management process to address social media risk?".

Information: Sociala media kan användas av människor för att utbyta information eller innehåll, samarbeta och för en hel del mer. Exempelvis vanliga media som nyheter på en TV ger inget utbyte mellan människor medan sociala medier låter användare kommentera, diskutera och dela nyheter. Frågorna nedan ska ses i sammanhang av din organisations användande och riskhanteringspraxis kring sociala media.

Intervjufrågor:

1. Vilka sociala medier används av organisationen?

2. Används sociala medier för att:
   - förbättra kommunikationen med kunder/användare?
   - för att skapa kundintresse/försäljning?
   - för att förbättra och underhålla erat varumärke?
   - för att utveckla nya produkter/tjänster?
   - för att rekrytera ny personal?
   - för att kommunicera med anställda?

3. Finns det någon riskhanteringsplan för att identifiera och hantera risker med sociala medier?

   Om ja, hur ser den ut? Tycker du att den är tillräcklig?

   Om nej, varför och tycker du att det borde finnas?

4. Finns det någon policy för användande av sociala medier på arbetsplatsen?

   Om ja, hur ser den ut? Tycker du att den är tillräcklig?

   Om nej, varför och tycker du att det borde finnas?

5. Övervakas sociala medier av organisationen?

   Om ja, hur och av vilken avdelning? Tycker du att det är tillräckligt?

   Om nej, varför och tycker du att det borde övervakas?

6. Granskas användandet av sociala medier av organisationen?

   Om ja, vem gör granskandet?

   Om nej, varför?

Tilläggsfrågor:

Anser du er mer reaktiva eller proaktiva?

Hur skulle ni kunna vara mer proaktiva?

Appendix 3 Different Risk Management methods

There are a lot of different methods/guidelines of carrying out risk management and some are presented below.

ISO 31000 Risk Management

ISO 31000 is a framework of guidelines to make a strategy for risk management. The guidelines are appropriate for all kinds of organizations and can be used by anyone that wants to manage risks in organizations [29].

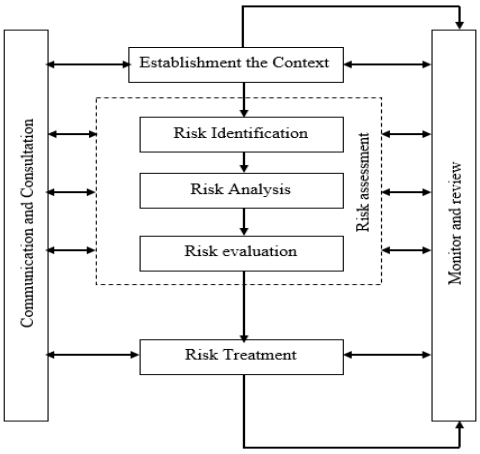

Figure 7. ISO 31000:2009 Risk Management process (Made from figure 1 in [11, p. 883]).

The first step (see Figure 7) in the Risk Management process is to establish the context, starting with a goal with the risk management process and what factors are included in the process. The risk assessment step includes risk identification, risk analysis and risk evaluation. The steps are done to find what risks are possible to occur and analyse these risks and evaluate how much attention should be put in depending on priority of the asset. Risk treatment step is the step where controls are set in depending on the earlier analysis steps [11].

ISO/IEC 27005 Information Security Risk Management

The International Organization of Standardization (ISO) [30]provides guidelines for information security risk management. The information security risk management process is recommended to be an iterative process and is described as containing the activities (see Figure 8): context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review.

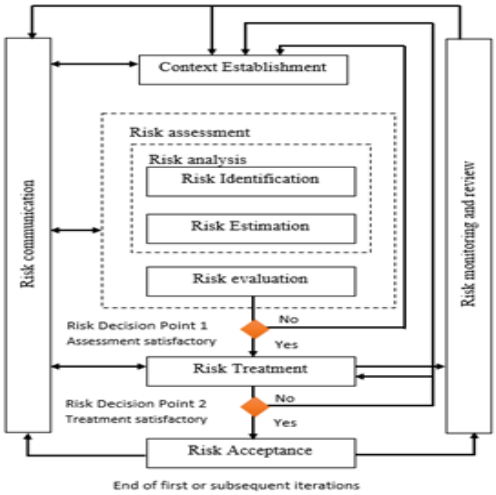

Figure 8. ISO/IEC 27005 Information Security Risk Management Process (Made from figure 1 in [30, p. 5]**)**

The context establishment is for defining what should be included in context of the risk management process. This activity also includes defining assets, threats and vulnerabilities. The risk assessment activity is for deciding what approach should be used in the risk assessment. The risk analysis should be used for finding threats, risks and what the likelihood and consequences of these would be [30].

The risk treatment activity is about how to manage the found risks and implement the treatment. The risk communication is about the risk being communicated to all involved. The risk monitoring and review is done to keep the process continuously monitored and reviewed. The risk acceptance activity occurs when the risks are at an acceptable level. This whole process can be done iterative to try to find as many risks as possible and keeping the assessment accurate [30].

OCTAVE Allegro

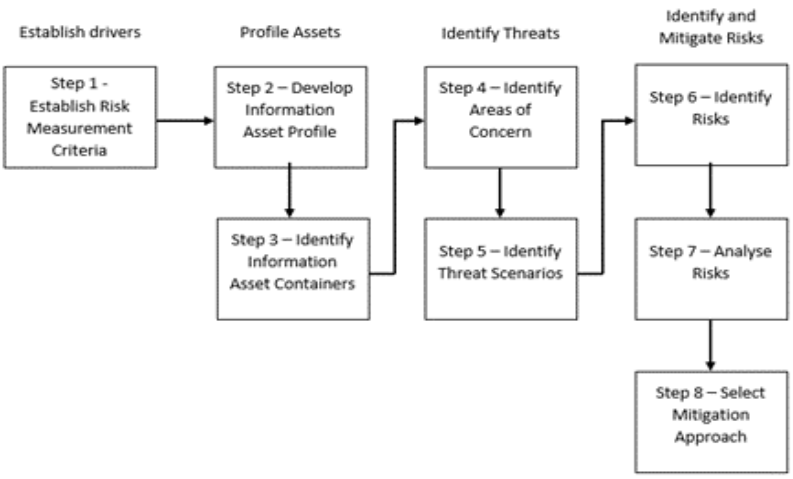

Figure 9. Octave Allegro steps (Made from figure 2 in [19]).

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro method helps organizations to perform information security risk assessment. OCTAVE allegro method (see Figure 9) is according to authors Caralli, Stevens, Young & Wilson [19] used to:

- Evaluate tolerance of the organization
- Find what assets that are important to the organization
- Find threats or vulnerabilities to the found important assets
- Try to evaluate consequences if the found threats would occur.

Enterprise Risk Management (ERM)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) have developed a framework called *"COSO Enterprise Risk Management - Integrating with Strategy and Performance"*. ERM is described by [31] as managing risks with the help of enterprise culture, capabilities and practices more than just treating risk management as a function of one department. The ERM consists of five components that are:

- **Governance and culture: t**he organizations structure with missions, visions and core values when it comes to responsibilities in risk management but also handling desired ethical values and behaviours in the organization.
- **Strategy and Objective-Setting:** how the missions, visions and core values should be integrated into the organization's strategy. Goals are also set to be able to identify and respond to risks.
- **Performance:** identification and assessment of risks, prioritizing them and then a response is triggered.
- **Review and Revision:** checking the performance of the risk management and if changes or improvement are needed to be done.
- **Information, Communication and reporting:** continuously collecting and sharing risk information in the organization [31].

A Business approach to Risk Assessment and Risk Management

The business approach by [34] is a development from the traditional risk management. The authors describe that classifying risks should be done by the effect they have on the organizations processes (confidentiality, integrity and availability) and not by the original approach that is based on the threat and vulnerabilities to assets (see Figure 10).

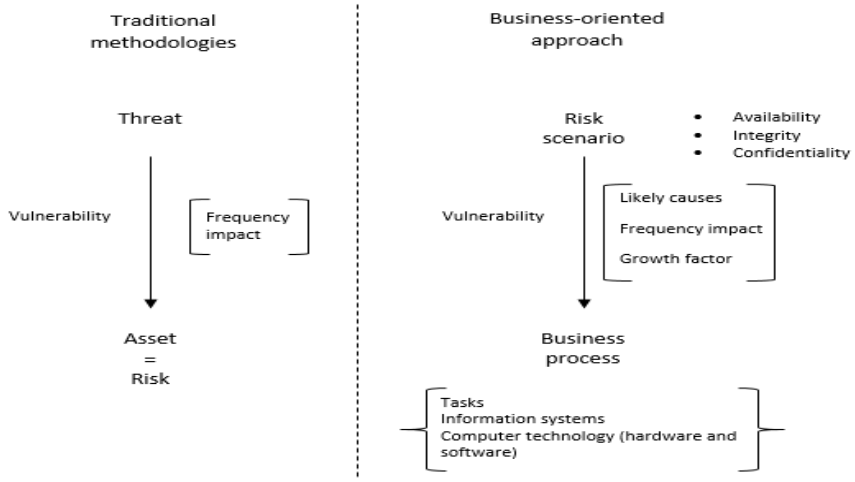

Figure 10. Traditional Risk Management versus Business Oriented approach (Made from figure 8 in [34]).

The approach suits smaller organizations and should be a lot faster and simpler by not performing an analysis of all IT assets but focusing on what processes are critical for the organization operation. Management sets the level of risk that is acceptable and when and how risk must be handled by criticality. The different countermeasures for the risks are accept/retain risk, transfer risk, avoid/prevent risk and control risk:

- **Accept/retain risk**: these risks have low impact and not so likely to occur. The cost for countermeasures is often exceeding the cost of the risk.
- **Transfer risk**: these risks have high impact but not so likely to occur, like for example earthquakes. A common way to transfer risk is by insurance.
- **Avoid/prevent risk**: these risks have a high impact and very likely to occur, so they need to be prevented as far as possible with for example access control for preventing information theft.
- **Control risk**: these risks have a low impact but are very likely to occur, for example errors need to be controlled with some kind of detection.

The authors emphasize benefits with a business-oriented approach, for example it saves cost, time and resources as it does not go into great detail in its analysis.