LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

A Risk Analysis of Social Networking Services for a Small Enterprise:

A Case Study of Conclave

Soebhektie, Sabrina

2016 Laurea Leppävaara

Laurea University of Applied Sciences
Laurea Leppävaara

A Risk Analysis of Social Networking Services for a Small Enterprise: A Case Study of Conclave

Sabrina Soebhektie
Business Information Technology
Bachelor's Thesis
March, 2016

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Business Information Technology

Soebhektie, Sabrina

A Risk Analysis of Social Networking Services for a Small Enterprise: A Case Study of Conclave

Year 2016 Pages 43

In the millenials era, social networking services have been a fundamental elements in people's lives, as social networking sites are able to connect people, help them get updates from around the globe, and also makes their lives easier by providing other functions. As a new startup company in Indonesia, Conclave has been using social media as core tools for their business activities. Nevertheless, despite the advantages of using social networking sites, these also may have security breaches that needed further attention.

The purpose of this thesis project was to identify threats on using social networking sites, pinpoint the vulnerable data that have the highest risk, and find the solution to minimalise the risks that may occur from using social networking sites for business purposes in the workplace according to the risk assesmen. In order to achieve the objective of the research, the writer has done a literature review, collected data, and analyze the subject of information security and risk assesment more deeply.

After doing the research, the writer has generated a risk assesmest result, and found that several social networking services have the risk of jeopardizing the company. That being said, the writer is establishing a various suggestions in order for the personnels of Conclave to be more aware of the importance of information security on using social networking services in the workplace.

Table of contents

Introduction

1.1 Thesis Introduction

Tang Lei (2010) describe a social network as a social structure made of nodes and edhes that connect nodes in various relationships. Social networking service have taken a major part in people's lives, notably with millenials or generation Y, who were born on and after 1998, came into an emerging world of technology and have grown up surrounded by gadgets (Gibson, 2003).

From that fact, companies have come to the realization of the importance of the presence of internet access, and the use of social media as communication and marketing platform for their future business development. Companies can easily engage with their customers with the fast and low cost method by using social networking service. The great benefit of using social networking service as the marketing tools is that the company can measure their success by leads and customers, rather than the more traditional web metrics (Barlow 2014).

Although social networking service have a great power of bringing advatanges for a company, but also can caused jeopardy as well as break a business or brand, no matter how big or small a brand is. The constant use of social networking platform that is keep growing, create the needs to analyse the security and privacy risks from utilizing it. With an access to an information network that is directly connected to your target audiences, it's the company's responsibility to ensure that everything that came out from them doesn't open up their company to a disaster (Sorisi 2014)

S.M. Furnell (2006) explains in his research, that it has been proven that the major contributor to security incidents are human errors and lack of awareness of security issues. Human error is defined as a failure of a planned action to achieve a desired outcome, and when poorly managed can increase the likelihood of an error occurring in the workplace (NOPSEMA 2015). The way to prevent human error occuring in the workplace is to educate the user, to make sure they have the required knowledge of information security and skill to act appropriately.

The objective of information technology, according to BSI standard 100-2, is to protect informartion of all kinds and from all sources. The classic core principles of information security are, confidentiality, integrity, and availability, also known as the CIA principles. Additional generic terms used in information security include, authenticity, validity. Reliability, and non-deniability.

1.2 Company Background

Conclave is a co-working space located in the centre of Jakarta, Indonesia, Whom offers a stimulating work environment with complete office facilities for freelancers, start up companies, entrepreneurs, as well as other creative industry's worker. The aim is to have a great working atmosphere to exchange ideas, to learn, and give people the ability to work inside a cubicle in an office space. The co-working space also includes meeting room, auditorium, library, recreational room, and also a virtual office, for start up companies that needed a postal address, as described in figure 1.

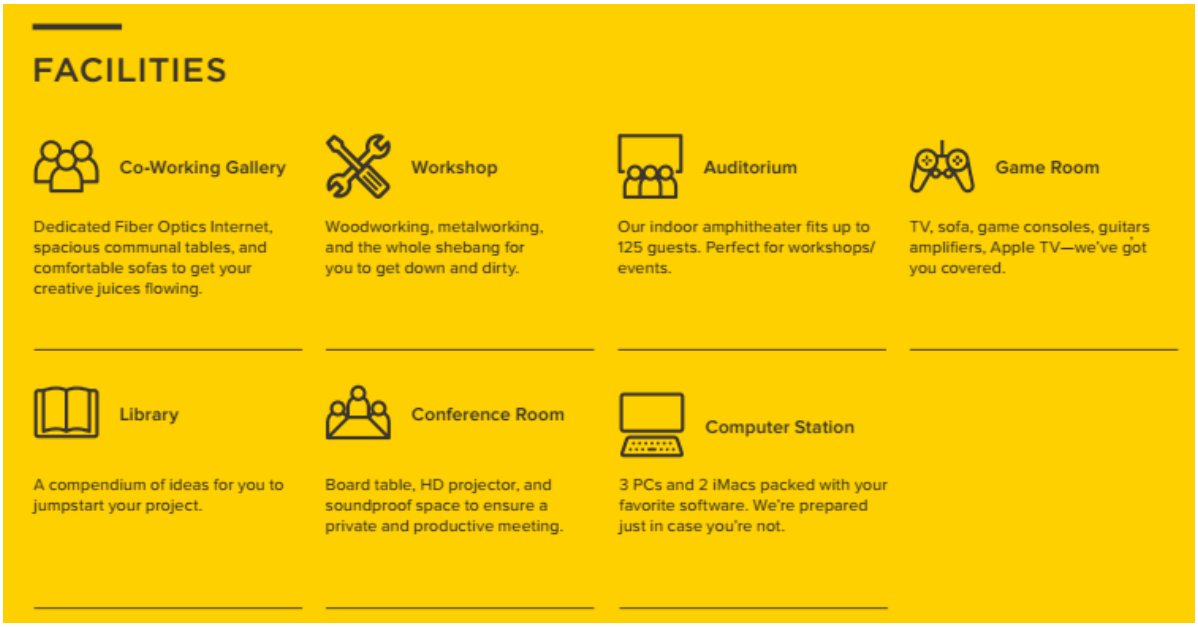

Figure 1: Conclave's Facilities

Conclave was formed in Jakarta, Indonesia, it is run by Gudang Kapital International Corporation. The company is led by Reynaldi Latief as the chief executive officer (CEO), Aditya Hadiputra as the chief financial officer (CFO), Akbar Maulana as the chief operating officer (COO), Bradhika Ayodya as the chief marketing officer (CMO), and two commissioner, Tita latief and Marshall Utoyo. There are around 200 new members monthly, ever since Conclave was open for public on Dec 20th, 2014.

Conclave mostly uses social networking service as a tool for their marketing campaign, a communication tool to be in touch with one another, such as for virtual meeting, storing their datas, and also as a research tool for observing their business scope development in the future. Thus, conclave needed to be fully aware of the need to protect system resources and the impact of human error on using social networking service in workplace.

1.3 Research Problems, Background, and Objectives

The author of this thesis was formerly work as an intern for Conclave, in early 2015. Thereupon, the writer was involved in a discussion with the human resource department of the company about the big amount of usage of social networking service on their business activity, which later on conclude how little the company knows about information security on using social networking services, as it is not commonly discussed in Indonesia. Subsequently, the writer notices that information security training is still very uncommon among companies in Indonesia, predominantly among start up companies who uses the social networking service most for their businesses.

The objective of conducting this research is to discover a variety of threats that may occur when using social networking services in workplace, in order to take a preventive measure to protect the vulnerable data and to minimize the possibilities of the occurement. And also to give the company the current data of the level of awareness amongst its personnel, which later on can be used for the personnel training in the future.

1.4 Scope and Limitation

This thesis will be focusing on finding a way to analyze and clarify the activity on using a social networking platform at workplace, and discover the risk that may occur. The research interest will be on helping the case company to optimize the use of social networking services with a less possibility of the data being damaged or threatened. This research is specifically concerning on the topic of human error, threats on using social networking sites, and risks that may occur during the usage of social media. The author of this thesis is emphasizing on being familiar with the risk assesment process in order to be able to understand more about the subject of this research and to be able to acquire the best result.

The author of this thesis will only be focusing on the the social networking sites that are uses by Conclave, which are, instagram, facebook, skype, twitter, google+, as well as cloud storage services, such as, google drive, and dropbox. There will also be a time limit for this research, considering the author of this thesis is expected to graduate on Spring 2016.

2 Theoritical Background and Knowledge Base

In this chapter, the author of this thesis will elaborate more on the theoritical background to give a better understanding about the topic of social networking service, risk management, and information security. The writer uses the following topic as the base of this particular research.

2.1 Social Networking Services

In this chapter, the author of the thesis will discuss more about the social networking platform. The purpose is by having a deeper analysis regarding this issue, it will help the author to examine the risks and threats for the case company on using it for their business necessity.

Lenhart and Madden (2008), define social networking site as an online place where a user can create a profile and build a personal network that connects them to other user. For modern society, social networks has been a fundamental part of one life as an online news distribution and consumption. Social media is one of the most powerful medium of present time, because it provides the ease and speed that enables people to create and distribute content (Agresta, 2010).

B. Bonin Bough (2010) explained that, a social media is the concept where individuals can remove barriers between each other, and provide for a completely participatory society. The term of social media itself was introduced by James Barnes, a sociologist from england in 1954 (Freeman 2006). Social network sites is not just allowing individuals to meet strangers, but rather enable the users to articulate and make visible their social networks (Boyd & Ellison, 2007).

Social networking sites can be classified into various types according to its utility and the service that they offer to the users. The different types of social networking services are, personal networking, business networking, video streaming, data storing, entertainment communication, online purchasing, blogging, virtual worlds, photo sharing, geolocation sharing, audio sharing, and news.

In the following subchapter, the author of this thesis will explain in more detailed about social networking sites.

2.1.1 Brief History of Social Networking Sites

Social network has developed through out the years of its existance. It was starting during 1950s with a telephone, the technology called phone phreaking. Phone Phreaking is a term for the rouge searching of telephone network (Borders, 2010). It was evolving over the years, which then the public saw the appearance of email in the 1960s, although the internet was not accessible to the public yet until early 1990s (Borders, 2010).

As described in the figure 2, The first social network site that emerged to the public of internet user was SixDegrees.com that was launched in 1997. The site authorize users to create profile, make a list friends, and becoming friends with other users. SixDegrees claimed their service as a tool to connect with other people. Despite the fact that SixDegrees had millions of users, the service discontinued on the year of 2000.

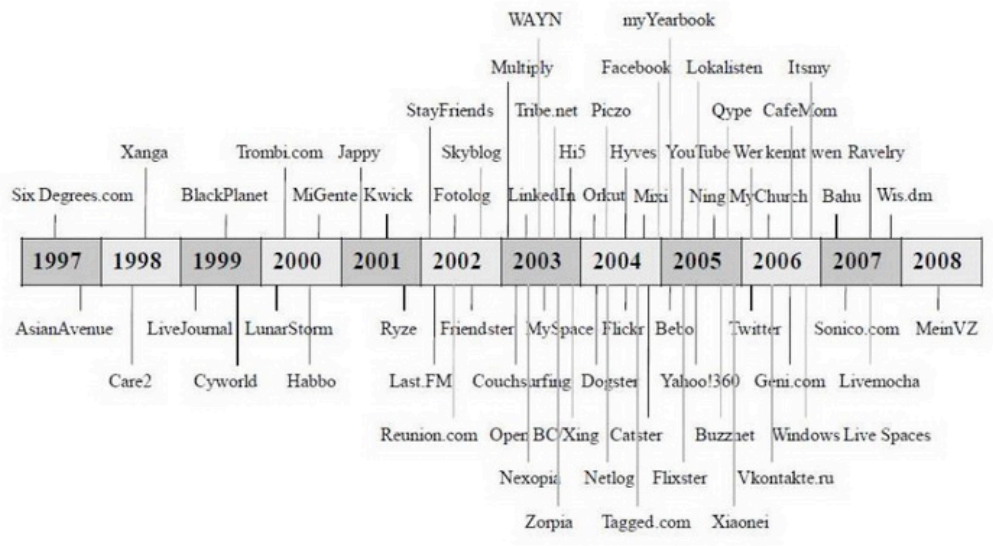

Figure 2: The Journey of Social Media (Heidemann, 2010)

Following the SixDegrees, there are a few of other social networking sites that appearing to the public, such as, AsianAvenue, BlackPlanet, and Migente, whom give permission for users to create a personal, professional, as well as dating profile, and add friends to their profile.

In 1999, a social networking sites called LiveJournal came out. Different than the previous social networking services, LiveJournal promotes their users to follow one another's journal, and the users can also manage their preference privacy settings.

The next trend of social networking sites is World of Warcraft, which is a Massively multiplayer online role-playing games (MMORPGS), who became a new genre of social network. MMORPGS allows users to interact in the game world, as well as on related forums, and community posts. This new trend of social network became very popular in the early 2000s.

Early 2000s is the era where more social networking sites are starting to coming out and ready to be used by the internet user. The most well-known social networking sites that was founded in the ealy 2000s are Friendster, Hi5, LinkedIn, MySpace, Facebook, Youtube, Multiply, Flickr, Photobucket, and other major social networking sites. The mentioned social networ-

king services were used to only allow users to connect with their friends, on 2006, Twitter was founded and create a new phenomenon of using social media, which is by having a real-time updates. The movement was then followed by other social networking sites, such as, posterous and tumblr, and by today, nearly every social networking sites has allowed users to post a real-time updates as a status.

At the present day, there are numerous amount of social networking services that are available to use. There are a lot more categories of social media that a user can choose, starting from streaming platform, platform for business purposes, e-messaging platform, dating platform, online shopping platform, and more other platforms.

2.1.2 Social Networking Services for Business

Currently, social networking services are not just used for entertainment purposes, but also for business use. The presence of social networking sites in the business world has changed the traditional method of business development. There are various ways for a company to utilize social media platform for the use of their business acitivity, which the process can be divided by two different objectives, an implementation inside the company, and outside the company (Puzyrnyy, 2011).

There are several ways of utilizing social networking sites for business implementations inside the company. For instance, a company could use social networking services as their communication tools between employees, long-distance meeting with clients, storing datas on cloud services, purchasing products, and many others. Currently, the use of information system using social networking services has become an essential component for big and small enterprises, and the innovations in the area of social networking sites for business purposes are rapidly developing.

For an implementation outside the company, social networking service is also has numerous benefits that can be used by the company to improve their business establishment. The most recognized utility of social networking service that many company has been doing is using the social media platform as their marketing tools to get in touch with their customer. Other ways to use social networking sites for business operation outside the office are for company branding, for market research, and also to recruit employees.

Social networking services are an exceptional tool as a company's bridge to the customer, because social networks provide a great way to understand the online customer's mindset. It can gather like-minded crowd around an external force of common interest, which can be very helpful for a company to amass their target group of people. Social networking services

are also makes it easier for enterprises to promote their product, as the tagging and sharing feature can help to spread the information faster. As the word spread around, it will also add further potential business value to the company (Brogan, 2010).

2.1.3 Social Media Concerns

The two most distinct concerns about the usage of social networking services are the privacy and security issue. In the generation where people tend to share almost everything in their life, there has been numerous cases of privacy violation of people who uses the social networking sites. In social networks, there are substantial amounts of problems that the users had to faced when other users release their information to public, the are many motives for this privacy breach, the reasones includes gossips, defamation, and also careless sharing (Markatos, 2011).

The difference between a security issue and a privacy issue is that, a security issue happen when a hacker gains an unauthorized access to a site's protected coding or written language. On the other hand, a privacy issue does not necessarily require security violation. (Collins, 2008). Brendan Collins (2008) also stated that these potential damage are depending on how much a user access a public site, and how much they share their personal information that can be harmful for the owner if the information got violated. The problem is individuals nowadays does not worry about the importance of the privacy from the information that they are sharing openly in public. As only very few of the internet users think about the damage that might occur after oversharing an information on a default openness. Tranberg, Heuer, 2013).

Simson Garfinkel (2000) explained that a privacy is human's right to control what detailes of their lives that can be shared to public, therefore, people should be fully acknowledge of who collects what information, and how will they use those information. By having facebook as an example, the default setting on user's profile is that everything they put in their profile can be seen by anyone. Although, user have the capacity to change their privacy setting to limit the viewer of their profile. The real risks in data vulnerability is the value of access to the information for cybercriminals (Clueley, 2009).

As for security issue, social media is a vulnerable and easy target for online criminals, or hackers to get into the users system, steal users' confidential information, and/or spread viruses to the victim. One of the various way to got into users account is by using a third-party services, that usually needed a registration in order to access a certain function. A user can use their available accounts, such as facebook account, or gmail account, to register to the

third-party service in which they can gain full access to the users personal information inside the accessible accounts.

Another common threat of using social networking services is the possibility of a cybercriminal to misuse or abused the connection or the information from the social networking sites, to use the account to spread spam or scam, and also spreading malware viruses.

As for the social media concerns on using it for business purpose, there are a few possible crisis that might damage the company which can be divided into to varietie: the one that happens within the organization, and the one that occur outside the organization.. For example, the most significant risk is the impact on the company's brand or reputation. As it has been discussed earlier in this thesis, people have the ability to openly share their opinion to public, and the company should be aware of the activity on social media regarding people talking about their business, therefore, if there is a damaging information that has been shared to public, the company can handle the damage faster. Another damages that can occur, are information leakage, data loss, and also piracy or infringement.

2.2 Information Security

In the era where technology has taken out a big part part of people's life, information security had also become the important aspect and concern of computer users. The main purpose of information security is to protect various kinds of company's information, assets, and operations (BSI Standard 100-1). Information security is used to protect information from a wide range of threats in order to ensure business continuity, minimize the damage for the business, and maximize the return of investment, as well as business opportunities.

Dependency towards information security is growing, as the level of the potential threats are increasing. Information security can be approached with three main principles objectives; confidentiality, integrity, and availability (Ahmed, Sharif, 2012). Confidentiality is the property that an information is not made available to everyone, only an authorized individuals can have an access to the informatin (ISO 27001). Integrity principles has a value of an information can only be modified, or changed by an authorized person and with an authorized manner, and availability princioles have a meaning of the information is only accessible upon demand by an authorized individual (Alexander, Finch, 2013)

Information security can be achieved by implementing a set of control or safeguards, which could be in the form of policy, practice, procedures, organizational structure, and software function, the established safeguard is needed to ensure the specific secuirty objectives of the organization are connected (ISO/IEC 27002).

Information security has several sub-areas to focused on. The sub-areas of information security has a wide range of scope, and it has various way to approach different sectors. All of the development activitiy and maintenance of information security are directed to those sub-areas. The sub-areas of information security covers the subjects of administrative and organizational information security, personnel security, physical security, telecommunication security, data security, computer security operations security, software security, and computer security.

Information security is a business problem, theefore, the entire organization must contribute in solving the security problem based on its own strategy (Vacca, 2009). Inside every organization or company, there is a specific management function in which referring to the manager itself and the task process that the assigned person is doing. A management system contained of the policies that has a purpose of achieving the company's objective. The part of management system who are dealing with the information security related issue is referred as the information security management system (ISMS), who has the task to assign the instruments and method aimed at achieving information security.

The ISMS have four essential components, it includes, Management principles, resources, personnel, and information security process. Information security process has a lifecycle in order to breakdown the dynamic of the process, which can be divided into four cycle, planning, implementing the plan and conducting the project, performance review and monitoring the achievement of objectives, and the last part of the cycle is to eliminate the flaws that has been discovered and improve the current working strengths. This lifecycle is called the PDCA model, which named after the individual phases, "Plan, Do, Check, and Act" (BSI Standard 100-1), which can be seen in more details in the figure 3. The PDCA model can help to describe and examine the lifecycle of information security policy, and the information scurity organization.

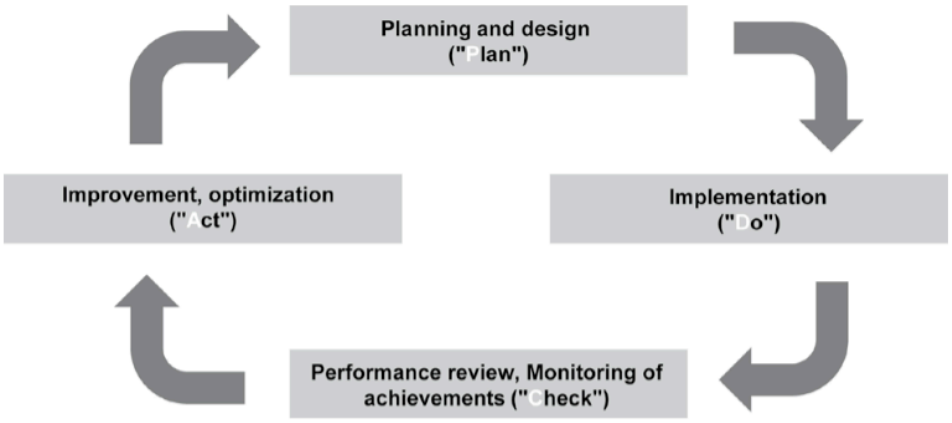

Figure 3: The PDCA Model of Lifecycle (BSI Standard 100-1)

The planning cycle is when the management analyze the current and upcoming condition on threats, determining the objectives of the threats, and developing the security strategy. The implementation or the ”Do” phase is when the security strategy is executed with the support of security concepts and the appropriate structure for the company. Since every organizations and company has a different conditions, requirements, and resources, the procedures should be adapted according to the company’s own needs, and the company can decide how the strategy that is more suitable and appropriate for the company.

On the next phase, which is the ”Check” phase, the management should have a regular inspection on the implemented strategy, and determine whether the implemeted strategy and concept is efficient and effective for the company. The last phase of the lifecycle model is the ”Act” phase, in this phase, the result from the previous phase has been reviewed, and have been decided on which to improve and which one is supposed to be optimized.

The information security process is a contionuous process, in which means it should be regularly assesed on a period of a time by the management, in the form of internal audit in order to maintain the effectivity of the assigned safeguards. In addition, it will also be necessary to do information security training on regular period for the employees.

2.2.1 Risk Management

According to NIST 800-12, risk assesment is one of the main activity in order to do a risk amnagement, it will help form the foundation of a well-constructed security management system. Risk management, as shown in figure 4, is the process to evaluate risks, finding a method to reduce the possibility of the risk, and maintaining the safe level for the risk. Risk management is formulated by two primary activities, which are risk assesement and risk mitigation, Although, an underlying risk analysis is also a fundamental activity in order to do a risk management. Risk management is a result of people that has recognize a variety of threats to their interet and thake precautions to protect them and to minimize the repercussion of the threats (NIST 800-12).

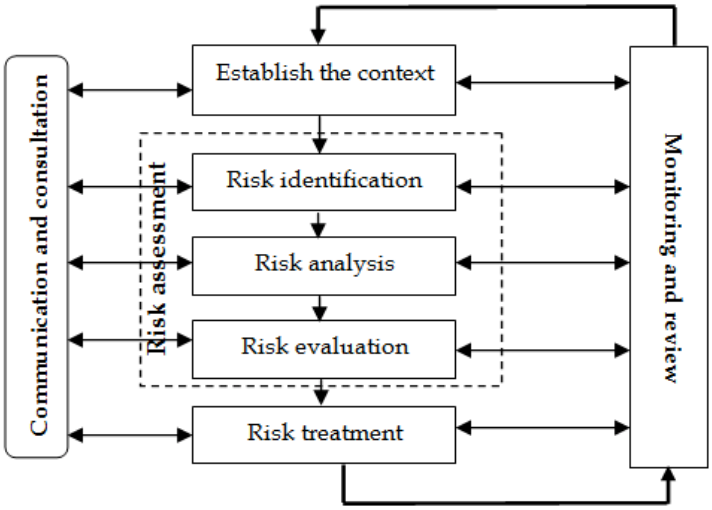

Figure 4: Risk Management Process (ISO 3100)

Risk assesment is the procedure of analyzing and interpreting a certain risk. The process is divided into three fundamental activities; determining the scope and methodology of the risk, collecting and analyzing the relevant data, and interpreting the risk analysis result. Defining the boundary, scope and methodology for the risk assesment will be affecting the total amount of effort that is spent on doing the risk management, it will also influence the type and usefulness of the assesment's result (NIST 800-12).

The risk assesment is needed because it will help the recognition of the risk, and to help the selection of the most effective controls as the outcome. Some of the most common security risks are, USB storage devices that is used for storing sensitive company data, a remote control softwares, work email that is used for exhanging sensitive information about the company, general internet use, office's laptop that stored company's information and data, and peer-to-peer application, as it can carry a malicious viruses that can affect the whole company's system.

In order to do the risk assesment, it is needed to identify the threat. The threat identification is necessary, since, it will help determine the probability of the occurance of the threat and their potential to harm the company's confidential assets. Even though, the risk analysis should concentrate on the threats that are most likely to occur and have the biggest impact on the livelihood of the company, it should also investigate the area that are poorly understood, and new.

According to BSI Standard 100-1, there are two ways to classify a threat; by looking into the orientation to damage scenario; as for examples, financial consequences, violation of laws, etc., and the other way is to define the classification of protection that is required in order

to reduce the risk. The classification of the protection against the effect of a threat can be divided into three catagories, which are normal level of protection, high level of protection, and very high level protection. The risk can be putted into the classified level of protection by analyzing the impact of the threat itself, which can be seen in the figure 5. This catagorization can be done by doing the consequences assesment, in which the company can estimate the degree of damage or loss that might occur (NIST 800-12). The specification on classifying the protection also affected by the size of the company.

Level of Protection	Impact of the Risk
Normal	Loss or damage is limited and calculable
High	Loss or damage may be considerable
Very High	Loss or damage can attain catastrophic proportions which could threaten the safety of the company

Figure 5: Classification of Protection (BSI Standard 100-1)

The next phase of risk assesment is to collect and analyze data, by doing a screening. Screening is a process of collecting more relevant information that can later be analyze, and the needed action can be taken sooner to control the limit of information gathering and analysis. It is necessary to do an asset valuation to documented the company's resources that might get an impact of the risks, which include, information, software, personnel, hardware, and physical asset, but only the threats that will have a significant probability that should be considered (ISO 17799).

The several step should be done to support the risk assesment to accomplish the desirable outcome, the risk assesment must have produced a meaningful and significant output that reflects what really is important for the company. The output of the risk analysis can also determine the action of treating the risks. The treatment actions towards the risks, includes, avoid or terminate the risk, accept or tolerate the risk, reduce or modify the risk, and transfer or share the risk (Alexander, Finch 2013). In this particular research, the writer was following the IT Grundschutz method in order to do a risk assesment according to BSI-Standard 100-1. According to IT-Grundschutz methodology, the three most crucial risk assesment processes are, structure analysis, assesing the protection required, and supplementary security analysis. The supplementary security analysis is only implemented if necessary, in which only appear when the company neeeded a higher protection requirements.

2.2.2 Personnel Security

Personnel security is one of the sub areas that are covered by information security management, it is the area of security that include all the standard and course of actions to help deciding whether an individual's employment is consistent with the company's security interest. The security concerns should always be taken into account when recruiting an employees, and also when monitoring the employees' work performance, because, human error is one of the major causes of occured incidents, on the other hand, it is inconceivable to separate human from the technology feature. The personnel security control that can help the company's ability to mitigate risk within the individuals are including, personnel screening, security responsibilities, terms and conditions of employment, training, raising awareness and recourse (ISO 17799).

Personnel screening is the process in which the company give the employee the policies according to the legal framework concerning company's assets. A security responsibilities is procedure where the company explain to the employees about their information security responsibilities, which can includes non-disclosure agreement, and codes of conduct. The terms and conditions of employment is when the employees are informed about their information security responsibilites as a part of a condition for their employment contract. It is important that, the company ensure the employees' accountability of the information security policies through training programs, and other way, such as making a requirement where the employees needed to make an acknowledgement statement which state that the employee has read and fully understand the information security requirements.

Information Security awareness' training is necessary to be conducted for a new employee, and also the established employees. Enterprises that do not implement awareness training plan are more likely to experince a security related issue (Alexander, Finch, 2013). Information security training tends to be more focused on a certain specific information security issue, it is mainly aimed for the employees to achieve a certain level of competence in a given area. The main purpose of the training is to reduce error and negligence, as it will improve the employees' awareness towards the need to protect system resources by educate them on what they should know and how they should do it. The developed skills and knowledge that are gained from the training will be beneficial to the company as the user or the employees can perform their job in a more secure way, and also it will support the individual accountability regarding information security issues (NIST 800-12). The level of information security awareness training is also can be vary according to the company's needs, as long as the outcome will be sufficient to ensure that the employees can carry out the essential assurance procedures and have an enough understanding of the right was of using the information systems (Alexander, Finch, 2013).

The training is also essential because, awareness can help stimulates and motivates the employees that has been trained to be more careful about security and to also remind them of the importance of the issues. Awareness of the topic can be used to strengthened the fact that security can eliminate the possible failure in the company by protecting its valuable resources and assets. An awareness campaign or security training programme should be developed as a formal project with an agreed objectives by the management in order for it to deliver efficiently and measured for success. The security training should be done simultaneously on a regular period of time, athough, it is important to focus on the security issues that are relevant to the company's condition.

3 Research Approach

In this chapter, the author of this thesis will discuss about the process and method in order to analyze deeply the problem of this research, and to achieve the answer to the research question. The research methodology that the writer has chosen for this particular research project is the case study method. The reason that case study method was chosen is because, this particular research is exploring an actual situation on a deeper level, and this research topic uses a set of data collection techniques, and a specific approaches to data analysis (Yin, 2009). On this thesis, the author believes that the most suitable way in order to get the best results is to use a mixed method data analysis.

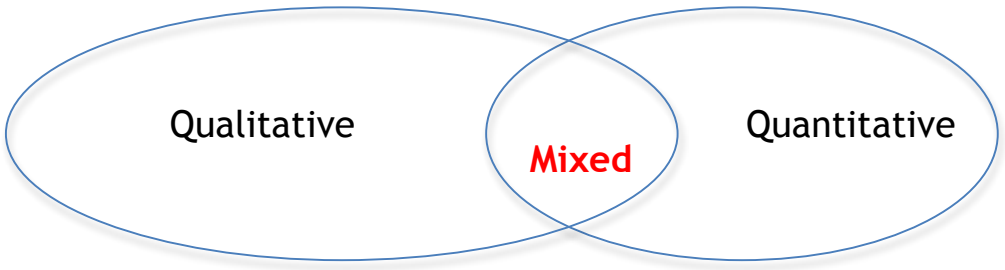

Figure 6: Mixed Method Data Analysis

According to Figure 6, It shows that a mixed method data analysis is a combination between qualitative method and quantitative method. The writer chose this data analysis method because qualitative research allows the writer to explore and get better understanding of the involved individuals, whilst the quantitative research let the writer to test the objective theories, the combination of qualitative and quantitave approaches can gives a better understanding of the research problem (Creswell, 2003). A mixed method approach is when the researcher base the knowledge claims on a practical grounds (Creswell, 2003). The applied

methods that are suitable for this certain research are, interview, questionnaire, and analysis.

To be able to execute a case study method, the author needed to make a research design. Robert Yin (2009) define a research design as a plan for getting a conclusions and answer to a set of questions. Although, there are five components of a research designs, the three most important points are: a study's questions; the propositions; and the units analysis, The plan is also supposed to be able to help the researcher to determine the next step of the research after the data has been collected. There are four major criteria to conclude the quality of a research design, which are: construct validity, internal validity, external validity, and reliability.

In the following subsections, the writer will describe more distinctly the approaches, and methods that are used during the research phase of this thesis.

3.1 Data Collecting Method

The author of this thesis has chosen several methods in order to get a better understanding on the hypothesis of this research. Since this thesis is a case study of Conclave, the writer will go in depth the activity of the company. As Robert Stake (1995) explained, the researcher of a case study should collect detailed informations using a variety of data collection procedures over a continuous period of time. In addition to that, the writer is following the instructed risk assesment methodology that was adapted from IT Grundschutz in BSI-Standard 100-1. According to the Federal Office for Information Security website, IT Grundschutz is an IT baseline protection procedure that was made by the German Federal Office of Information Security, which helps organization to execute computer security act.

The writer will obey the sequential procedure strategy on choosing the research method. A sequential procedure is when the researcher combine the findings from one method to another. As in most cases, the researcher begin the analysis with a qualitative method for finding facts, and followed by quantitative method so the result of the research can be checked (Creswell, 2003).

The different methods that are applied for this research are, literature review on the specific area of risk management, interview with the human resource department of the company, and handing out questionnaire to the employees of the company. The outcome of the research methods above will be the foundation of the final outcome that the writer will make later on in this thesis. The author will explain the research method in more detailed on the further subsections.

3.1.1 Literature Review

According to Explorable, a literature review is an analytical evaluation of a certain research. A literature review should be able to help the researcher to give a theoritical basis of the fact-finding phase, obtaining the pre-understanding of the specific topic, determine the nature of the research, and help narrow the research area, as shown in figure 7.

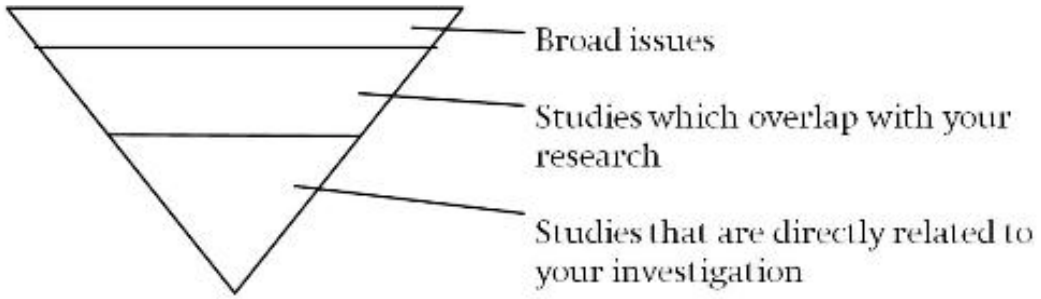

Figure 7: Benefit of Literature Review (www.reading.ac.uk)

For this research method, the author of this thesis has to do four stages in order to do a further development. The first stage is to sort the crucial problem for the research, which followed by finding the literature that can help the researcher to find the relevant material, the third stage is to make data evaluation to determine which data is important for the topic, and lastly, making a conclusion of the material that has been gathered from the literature. Based on the literature review, the author of this thesis will adapt and follow the risk assesment process in order to analyze and get the best possible outcome of the objective from the case condition.

3.1.2 Interview

An interview is a research method that is conducted to find meanings from the insight information of the interviewees. An interview is useful for getting an in-depth information around the distinct topic from the participant (McNamara, 1999). Alike the previous research method, interview also can help the researcher to get a better understanding of the research topic.

There are several different types of conducting interviews, and for this research, the author of this thesis did an unstructured interview. An unstructured interview is a way of understanding the complex behaviour of people without imposing any categorization, which might limit the depth of the subject matter (Punch, 1988). During the development process of this re-

search, the author of this thesis conduct one interview with the Chief Operating Officer (COO) of the company, Akbar Maulana, whom also in charge of the human resource department. The interview is aimed to collect the perspective of the COO about their desired outcome of this research, and to acquaire the background knowledge of the particular topic from the management point of view.

The author of this thesis has also attached the entire interview in the following Appendix.

3.1.3 Questionnaire

A questionnaire or a survey research is a collection of gathered informations from a sample of individuals through their response to a given question. Survey research method provide a quantitative description of an opinions or attitudes of a group of people by studying the sample of the population (Creswell, 2003). The content of a survey or a questionnaire should be clearly defined based on the background research for it to be valid (Andres, 2012),

The survey that the writer conducted for this research is given at the 11th of November 2014, to ten of the employees of Conclave through the human resource department, who then authorize the survey by checking the content of the questions beforehand. The survey was conducted via Google Forms, which is an online survey service platform powered by Google. The identity of the participants are anonymous. Within two days, the researcher was able to get a sufficient amount of answers from all of the employees of conclave, which then help the writer of this thesis to be able to analyze the result and give the outcome that has been discussed.

The questions in the surveys are concerning about their social media usage in the workplace, the employee's history of information security education, and also regarding their personal understanding in the topic of information security. The first four questions in the questionnaire, are regarding the type of social networking services that they use in the workplace, whether they use it for business purpose or personal purpose, and also the determining which function of the social networking services are they using in workplace. These questions can help the author of this thesis to discover the various kind of prevention towards risks from different platforms of social networking services.

The fifth question on the survey is to inquire what types of content that the employees of conclave generally share on the social networking sites that they are accessing in the workplace. This question will be beneficial for the researcher to identify what kind of leakage of information that might occur from the employee's activity in the social media platforms. On the sixth question, the researcher is seeking to know the background knowledge of informati-

on security that the employee's have, whether they genuinely understand the aspect of information security. And on the last two questions of the survey, the researcher asked on the employee's background training in the field of information security, and spefically where did they got it, if the employee have had the regarding training. The quetions that the author of this thesis formed in the survey is to give the writer a brief knowledge of the kind of information security awareness that the employees of conclave needed to get in the future.

The author of this thesis will discuss about the result and findings of the questionnaire on the following chapter.

4 Data Analysis

As following the risk assesment procedure, after the research has determined the scope and methodoly, and have also collected the relevant data for the analysis, the final phase is to comprehend the result of the data collection, which in this particular research, has been taken by a survey. The figures has been made to make it easier for the reader to understand, it was made using the built-in function from Google Form, which can calculate the percentage of the answers automatically. The results have been divided into sub-sections according to relevant subjects.

4.1 Question 1: Social Media Platforms

Different kind of social networking services is used in the workplace, for different kind of purposes. In the survey, the writer asked the participant to answer which of the listed social media platform they are normally use in workplace. The most used social networking platform that is accessed inside Conclave office area is Twitter (Figure 8), 24% of the employees of conclave is accessing twitter in the workplace. Followed by Facebook and LinkedIn which both accessed by 21% of the employees of Conclave. After that, 18% of the employees are using Instagram, and 9% uses Google+.

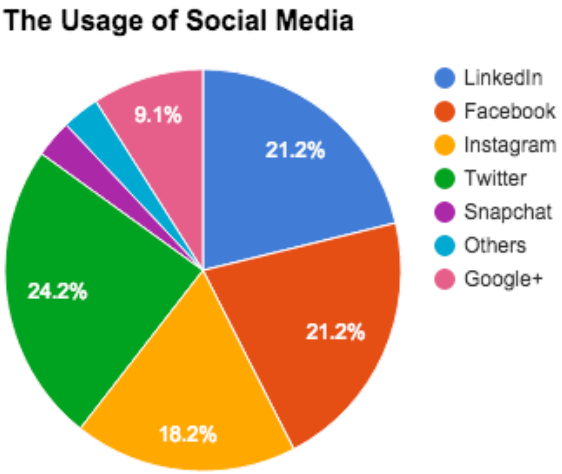

Figure 8: Social Media Usage

4.2 Question 2: Business Related Activity on Social Media

In the following question, the writer asks the participant to response to which of the listed activity on social networking services that the employees uses the platform for, the question divided by two different utilization, for business use, and for personal use. The data from the following question about the use of the social media for the business purpose, enables the writer to understand the importance of the utility of social medias for the business development of Conclave.

From the listed utilities, there are three main service that the employees uses (Figure 9). 45% of the employees uses social media as their communication tool. The second most used service is data storing, and followed by promotion purpose at 25%. As mentioned before in the theoritical review, the main purpose that most companies used for their business activities are for their internal communication platform, to reach the customer for their marketing use, and also using the cloud computing service as a data storage platform.

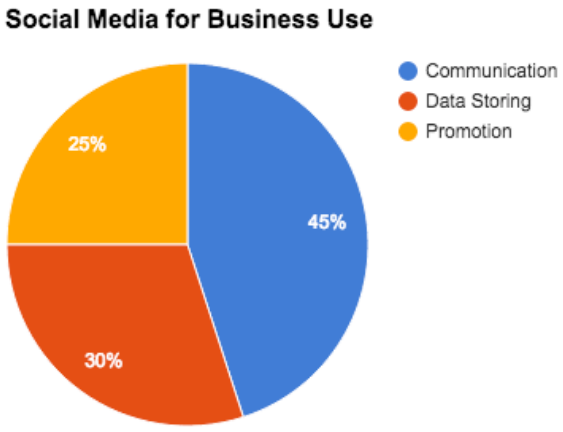

Figure 9: Social Media Usage for Business Purpose

4.3 Question 3: Personal Related Activity on Social Media

The result from the following question will help the author of this thesis to be able to give a recommendation of prevention that the management can take in order to prevent the threat that may occur from using social media for personal activities in workplace. This question can also enable the researcher to analyze the possibility of information leakage, and also the activity that may caused harm to the company system.

From the response that the writer got, which can be seen in the figure 10, 45% of the participants uses the social networking services for their communication tools, the result is the same as it was for the business purpose. The result of using social networking services for a video streaming tool, and for others activity that are not listed in the answer options, are both 25%. The other utility that the employees uses are for logging in to other sites, transferring data, and reading the news. The rest 5% of the answer from the participant is allocated for the online purchasing use.

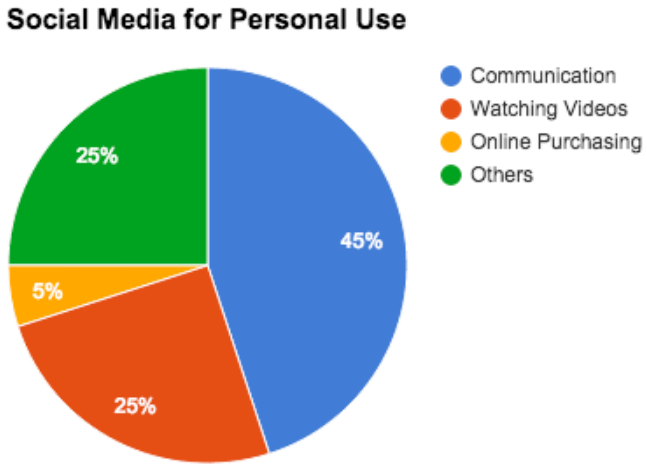

Figure 10: Social Media Usage for Personal Use

4.4 Question 4: Shared Content on Social Media

The next question on the survey, the writer inquired the participant to answered according to the given list, which of the listed content did they shared on their social networking sites, whether it is for business purposes or for personal use. The content that the employees shared can help to determine the possible vulnarable channel for an authorized individual to gain access to the company's information and/or data.

According to the answers of the given question, there are four mutual shared content on the employees' social networking services (Figure 11). The content that the employees mostly to transmit is text message in which 45% of the participant answered. This answer is plausable, given the fact that communication is the main activity that the personnel uses. 35% of the employees answered that they mostly share a picture on a social media. 15% of the participant answered Video, and only 5% answered othes. The other content that the employee shared in the social networking sites is document.

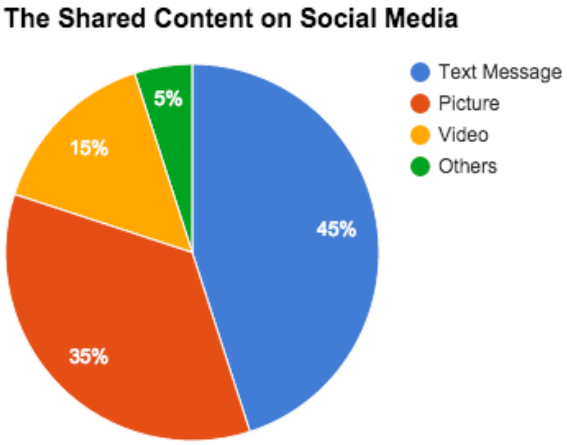

Figure 11: The Most Shared Content on Social Media

4.5 Question 5: Information Security Knowledge

The following questions that are given in the questionnaire is regarding the general background knowledge of information security amongst the personnel of Conclave. According to the conducted survey (figure 12), only 11% of the participant understand what information security is about.

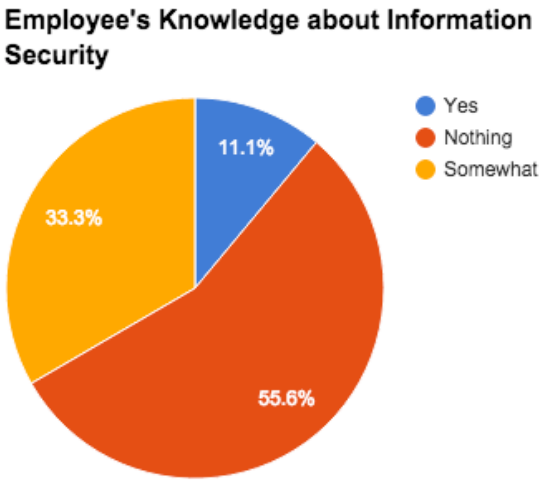

Figure 12: Background Knowledge about Information Security

The majority of the participant, which is 55% of them, answered that they did not know anything about information security, and 33% of the employees somewhat know what is the vague definition of information security. The participant does not given any available answer for this particular question, they are allowed to answer in their own writing. Only one of the employee can slightly describe information security, although still in a very indistinct way. Those who answered the question by somewhat, are describe the information security terms as "securing".

4.6 Question 6: Information Security Training Background

The next questions in concerning the history of any kind of information security training (Figure 13). Even though, by examining on the previous question, the answer for this particular question can already be predicted. 100% of the contributor answered that they have not been attending any form of training regarding information security topics. The answer to this particular question can be useful for the author of this thesis to specify which kind of basic knowledge and skill of competent that the employees needed to learn in their planned information security training. The response from this certain question did not surprised the writer, as, in Indonesia, Information Security training is still very uncommon in the business industry. Moreover, for a start-up company, although practically information technology has been use massively for the business activity in the past years.

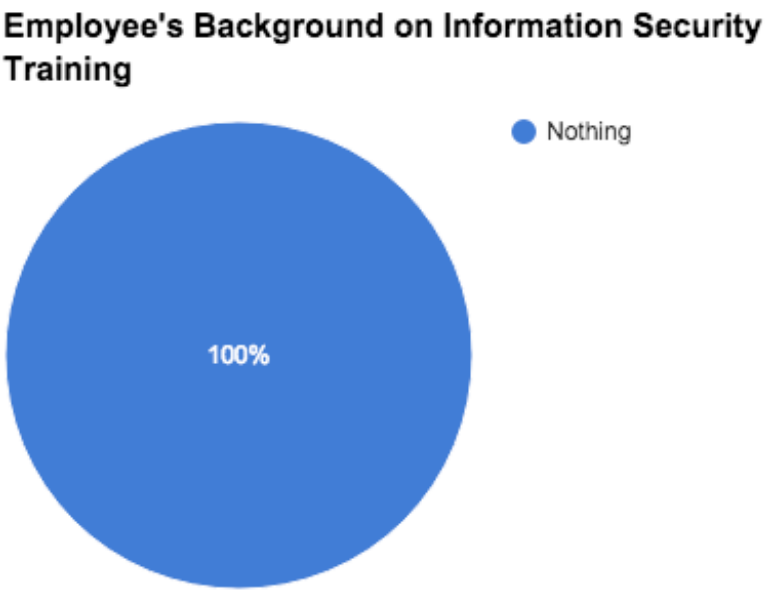

Figure 13: Employee's Training History

4.7 Interview with the Company's Representation

As previously mentioned, another research approach that the author of this thesis has conducted is having an interview with a representation from the Company. This sub section of the thesis will be consist of the summary of the conducted interview. The detailed transcript of this interview can be seen in the Appendix of this thesis. For this interview, the writer got the opportunity to have a discussion with the chief operating officer of Conclave, Akbar Maulana. This interview is conducted earlier on the 14th of October 2015, on an online voice call service via Skype. The interview covers the topic of his personal opinion towards information security awareness whether inside the company, or in the business industry scene in Jakarta, the writer, his personal social media use in workplace, and Mr. Maulana also discuss his desired result of this analysis, which he will use as an improvement tool for the company.

According to his perspective, information security topic is still very vaguely known in Indonesi, although, almost every living individuals in Jakarta have an access to internet. Owing to that fact, Mr. Maulana was very enthusiast when the author of this thesis approach him with the topic. He believes that information security knowledge is very important, moreover to the employees that has access to company's sensitive information. In spite of the fact that he has never seen any of the Conclave's employees overshared their working information, from his personal experience, he had seen several people openly shared an information and/or data about their work, which can be very dangerous if it was seen by the wrong people, and take the advantage of the important information or data. In his opinion, the people who has overshare their work details are simply not educated enough, and therefore, a training in relating to the subject is very important, and either a big or small company should have done the relevant training. He is confident that none of the employees of Conclave will mishandle the valuable information and data that has been given to them, but he believes that a prevention of a risk is better and more convinient, instead of fixing a problem.

Regarding his personal use social media in workplace, he admits he have also access a few social networking services in workplace on working hours. He normally uses the social networking services for the communication purposes, to read the current news, and also for refreshment purposes. Similar to the answer of the survey, he also uses Twitter the most in the workplace, since twitter can provide a set of news and information without having to access multiple sites. In his opinion, it is impractical to prohibit the employees from accessing the social networking sites in the office, as social medias has taken a big function in their business activity. According to him, social networking sites enables the user to connected with one another in an easy and effortless manner.

In the matter of the outcome of the research, Mr. Maulana expects that he will get a sufficient data of the current condition of employees level of knowledge towards the relevant subject, he also expect to gain a documentation on what kind of set of knowledge that he will need to convery to the other employee on the information security training ahead, as well as the final result of the research in the form of this thesis.

4.8 Risk Assesment Result

According to the the objectives that has been discuss in the earlier part of this thesis, the outcome of this particular research is to make an information security recommendation for Conclave that can be used as a guidance for a future human resource development project in the related issue, and also give the company the data of the current condition of the employees knowledge towards the information security issue that was already presented in the previous sub section. In this section, the author will describe the information security recommendation based on the interpretation from the analysis of results.

Platform	Content	Threat	Impact	Possibility	Risk Factor	Priority
Facebook	Messages Picture Video Marketing Content	Leaked information Malware Hacked Data loss	High	Likely	High	2
LinkedIn	Messages Marketing Content	Leaked information	Normal	Likely	Normal	3
Instagram	Picture Video		Low	Unlikely	Low	3
Twitter	Marketing Content Messages	Malware Stolen accounts Data piracy	Normal	Likely	Normal	3
Snapchat	Picture Video		Low	Unlikely	Low	3
Google+	Data Picture Video	Tracked location Automatically Geotagged Leaked Information Data infringment Data loss	High	Likely	High	1

Priority:
1 = Critical
2 = Marginal
3 = Negligible

Figure 14: Risk Assesment Result

In accordance with BSI 100-1, the first step of risk assesment is to identify the informations that needs to be protected, and also identify the possible threat for each and every informations. Therefore, after mapping the company's shared contents on social networking services on each different platform, the author of this thesis can divided the risk that can occur for different contents that was shared to other user. The author of this thesis has also compile

the result of the risk assesment according to the result of the survey, as can be seen from figure 14.

On Facebook, the employees of Conclave are usually sharing messages, news, and marketing or promotional content. According to those activity, the threat that have biggest possibility to occur are information leakage, data loss, and infringement of company's material. As for using twitter, which the personnel are most likely to share news and marketing content, the possible threat that can be found is data piracy. And the last social media that might have a crucial impact for the company is, Google+. The personnel are mostly using Google+ for their data sharing and data storing platform, which can lead to information leakage, data loss, and data infringement.

In compliance with the risk assesment that has been done, Google+ has the highest priority of supervision and protection, as the employee stores their data and sensitive information through the social networking accounts. Facebook is on the second place of the priority chart for Conclave's social media risk analysis, owing to the fact that, facebook has an impact of carrying malware, and also have had several cases of hacked accounts.

5 Results

After the writer has become familiar with the theoritical part of the research, the writer has been able to assemble a questionnaire. The purpose of the questionnaire is to help the writer to analyze the risk assesment according to the relevant data, and interpret the result of the risk assesment. There were ten participants of the occured survey, whom all are the employees of Conclave. All of the participants are familiar with the terms of social networking sites, and all of them are an active user of several social networking services.

According to the respondents' answer, the most used social networking sites in a workplace is Twitter, Facebook, and LinkedIn. The employees of Conclave are using the social networking services for both business and personal purposes. For the business purposes, 45% of the respondents uses the social media as their communication tools. The same result was appearing on the question about the usage of social networking services for personal use, that the majority of employees uses the platform for the communication purpose. Concerning the content that the participants normally shares on social networking sites, 45% of the employees respond that they mostly exchange text message, and 30% of the respondents share picture in their social media accounts.

The further questions are meant to discover the level of awareness towards information security that the employees have had. From all of the response, only a single participant who can

roughly answer the definition of information security. With reference of the previous question, the answer to the question of whether or not they have attend an information security training before, all of the respodents answer that none of them have any experience in any sort of training regarding the topic of information security.

The writer of this thesis has also performed an interview with a representation of the company. From the result of the discussion that they have, the representation of the company has the similar vision and point of view with the author concerning the topic of information security awareness. He also shares his view towards the information security issues that is happening in the present day. The representative have also made a point of refusing to forbid the employees to use social networking sites for personal use in the workplace. He expects to receive the results of this research, which then the relevant data and recommendation can be used for further development project for the company.

The writer of this thesis has put in writings all the information security recommendations in regarding to the employee's social networking services activity, that would be necessary for the current condition of employees' knowledge. The recommendation includes security software suggestions, as well as recommendation of action for the management in order to raise awareness towards the subject of information security.

The following recommendation are given according to the company need based on the employee's activity on social media. The first recommendation is for a basic prevention in regards to threats, because the human resource department refuse to limit the use of social media, it is advisable for the company to make a social media policy for the employee as the guideline of the limitation on the information that they can share on the internet, and also an example of the authorized manner to accss the social networking services in workplace, as the similar type of policy has been applied on most of the biggest companies in the world, for an example, Coca Cola.

The content of the social media policy can include the company's expectation of limitation in regard to the content that was shared by the employee which involve the company's information and data. It also includes the expectation of the company on how personnel behave while using social media within the work-related subject, as well as reminding the employees that there is a specific person whom has a specific task to be a representative of the company in the social media, and the particular person should always release a statement on behalf of the company, meaning that the information is not coming from the individual themself, and the person is fully responsible if they have released an unauthorised and inaccurate statement.

The second recommendation is to monitor the activity on social media that happens within the company. The company can hire a third parties to do the monitoring and reporting concerning this matter. The third recommendation that the writer suggesting is to allocate only a designated person to have the account of company's social networking sites, in that way, it is easier for the company to diminish the unwanted series of crisis that might occur. The company can make a separate non-disclosure agreement with the employee about the social media activity that the employee will handle.

The fourth recommendation that the writer suggested is to use a spam filter on email that is accessed using the work computer to prevent unwanted junk emails. The company should also recommended to uses a gateway antivirus, network-based security software that enables a detection on intrusion, monitoring to screen for the viruses attack and a attempts at security breaches by unauthorized user. In addition to that, it is advicable for the company to maintain its security patches by ensuring that the antivirus update on the work computer stays according to the schedule.

And the last and foremost recommendation for the company is to raise an awareness of the risk of an unmindful information security activity, by making an information security training. It is very essential for a company to raise their personnel's awareness towards an issue that involve a senstive information and document that can seriously harm their business.The company can execute the information security training by themselves, or hired a professional company that is specialized in the information security field to do so.

6 Evaluation

Although it was hard at first for the author to find a suitable topic for this thesis that fit into the standard of the previous thesis that has been published from the university, the work of this thesis is based on the personal concerns and interest of the author of this thesis towards the subject of social networking sites and the impact of using it in workplace. A few months in advance the author of this thesis has already approach the supervisor that the author thinks will have the same vision as she and have the best background on the subject, even before the author was supposedly starting the thesis writing period. The author was giving a few samples of idea for the thesis, and have a discussion with the future supervisor about each topics. After narrowing it down, the author of this thesis was able to do the research according to plan. The supervisor has greatly help the author to make a timetable for the thesis and the reasonable objectives for the research.

In the beginning phase of the thesis writing process, the writer has a problem of having to broad of a topic and objectives, which then narrowed down with the help of the supervisor.

The author of this thesis needed to have a large amount of literature review for the theoritical part in order to understand the topic in more details. The amount of background knowledge that the author of this thesis have had from the previous courses and projects in the related subject of information security has been very helpful in the process of comprehending the theoritical part.

In spite of the fact that the writer has a problem with a very tight plan schedule, as the author is planning to graduate in the spring semester, the author is very fortunate that the data collection process is considerably fast and easy, wih the cooperation with the company. The representative of the company is also very helpful and easy to reached whenever the writer needed to ask something or to inform the progress of the research.

Even though, there was some small issues along the way of the research and writing process of this thesis, the writer consider the process of creating this thesis is relatively smooth. The combination of the writer's passion and interest towards the subject, the background knowledge that the writer got from the study, and the help of the supporting figures of this thesis is what makes the process of making this thesis seems pleasant. The outcome of this thesis will be beneficial to the case company, as well as for the author to help her learn more about the subject that appealed the author.

7 Conclusion

This thesis was created to learn about the concept of the usage of social networking services in workplace, and to identify the possibility of threat occurrence regarding the activity. In the era where social networking services has taken a big part of human's life, social media has also been used in a numerous ways in the business sector. And although, using social networking sites has a plenty of benefits, it is also a window for harms. Therefore, it is crucial for a company to understand the risk of using social networking services, in order to protect their sensitive data from any harmful situation that may occur. Thus, this research was set out to allowed the writer discovers the possibility of an appearance of risks from the activity that involves using social media in workplace, and be able to find a set of preventions.

After the writer of this thesis has established the scope and methodology for the research, the writer continue to gather the important information and data that can be beneficial to help find the solution to the research question. After examining the relevant data, the writer has assembled a risk assesment result, that determine the possibility of risk occurence to the activities that associated with social media.

The result has shown that several social networking sites platform has bigger risk than the others, and a higher probability level of occurance. As a result, the writer has put together a number of recommendation for the company to be able to prevent any harmful incidents that may happen. The recommendations are including, social media policy, monitoring the social media activity that take place in the office area, uses gateway antivirus, spam filters, and also information security training, to raise the employees' awareness of the risk and possibility that might jeopardize their company.

References
Printed References:

Alexander, David, Finch, Amanda, & Taylor, Andy 2013. Information Security Management Principles. Swindon: BCS, The Chartered Institute for IT.

Agresta, Stephanie 2010. Perspectives on Social Media Marketing. Boston: Cangage Learning.

Andres, L 2012. Designing & doing survey research. London: SAGE Publications Ltd.

Boyd, Dannah M., & Ellison, Nicole B 2007. Social Network Sites: Definition, History, and Scholarship.

Brogan, Chris 2011. Social Media 101: Tactics and Tips to Develop Your Business Online. New York: John Wiley & Sons, Inc.

Carlson, Tom 2001. Information Security Management: Understanding ISO 17799. California: International Network Services.

Creswell, John W 2003. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. California: Sage Publications, Inc.

Edosomwan, Simeon 2011. The History of Social Media and Its Impact on Business. North Dakota: Minot State University.

Garfinkel, Simon 2000. Database nation: The Death of Privacy in the 21st Century. California: O'Reilly.

Guttman, Barbara, and Roback, Edward A 1988. An Introduction to Computer security: The NIST Handbook. U.S. Department of Commerce.

Lenhart, Amanda, & Madden, Mary 2008. Social Networking Websites and Teens: An Overview.

Lukka, K., and Tuomela, T.-S 1998. Testattuja ratkaisuja liikkeenjohdollisiin ongelmiin: konstruktiivinen tutkimusote.

McNamara, Carter 1999 General Guidelines for Conducting Interviews. Minnesota.

Pasian, Beverly 2015. Designs, Methods, and Practices for Research of Project Management. England: Gower Publishing Limited.

Stake, Robert E 1995. The Art of Case Study Research. California: Sage Publications, Inc.

Punch, K.F 1998 Introduction to Social Research: Quantitative and Qualitative Approaches. California: Sage Publishing.

Seidel, John V 1998. Qualitative Data Analysis, Colorado: Qualis Research.

Sorisi, Alex 2014. Social Marketing: The Complete Guide. London: Future Publishing Ltd.

Vacca, John R 2010. Managing Information Security. Burlington: Elsevier Science.

Yin, Robert K 2009. Case Study Research: Design and Methods. California: Sage Publications, Inc.

2009. ISO 3100:2009 – Risk Management. Geneva: ISO.

Online References:

Human Error. Accessed on October 2015.
http://www.nopsema.gov.au/resources/human-factors/human-error/

The History of Social Media 2009. Accessed on October 2015.
http://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/

Kasanen, E., Lukka, K., & Siitonen, A 1993. The Consturctive Approach in Management Accounting Research, Accessed on September 2015.
http://www.maaw.info/ArticleSummaries/Kasanen93Figure1ConstructiveResearch.gif

Write a Literature Review. Accessed on September 2015.
http://guides.library.ucsc.edu/write-a-literature-review

Collins, Brendan 2008. Privacy and Security Issues in Social Networking. Accessed on September 2015.
http://www.fastcompany.com/1030397/privacy-and-security-issues-social-networking

Barnes, Susan B 2006. A Privacy Paradox: Social Networking in the United States. Accessed on October 2015.
http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523

Burney, Aqil 2008. Inductive and Deductive Research Approach. Accessed on October 2015.
http://www.drburney.net/INDUCTIVE%20&%20DEDUCTIVE%20RESEARCH%20APPROACH%200603 2008.pdf

2011. Privacy Protection and ICT: Research Ideas. Accessed on November 2015.
http://cordis.europa.eu/fp7/ict/security/workshop-report-privacy-research-ideas-public.pdf

Ahmed, Munir, Sharif, Lukman, & Kabir, Muhammad 2012. Human Errors in Information Security. Accessed on October 2015.
http://www.warse.org/pdfs/ijatcse01132012.pdf

Shullich, Robert 2011. Risk Assesment of Social Media. Accessed on December 2015.
https://www.sans.org/reading-room/whitepapers/riskmanagement/risk-assessment-social-media-33940

The Coca-Cola Company. Online Social Media Principles. Accessed on January 2016.

http://www.viralblog.com/wp-content/uploads/2010/01/TCCC-Online-Social-Media-Principles-12-2009.pdf

The Federal Office for Information Security 2008. BSI Standard 100-1: Information Security Management Systems (ISMS). Bonn: *Bundesamt für Sicherheit in derInformationstechnik*.

The Federal Office for Information Security 2008. BSI Standard 100-2: IT-Grundschutz Methodology. Bonn: *Bundesamt für Sicherheit in derInformationstechnik*.

Figures

Appendixes

Appendix 1: Snapshots of Questionnare

Which of these following social media(s) do you use in workplace? *
(For business use)

- [ ] Facebook
- [ ] Twitter
- [ ] Instagram
- [ ] Snapchat
- [ ] LinkedIn
- [ ] Google+
- [ ] Other:

For what purpose(s) did you use your social media(s)? *
(For business use)

- [ ] Communication
- [ ] Data storing
- [ ] Promotion
- [ ] Online Purchasing
- [ ] Other:

Which of these following social media(s) do you use in workplace? *
(For personal use)

- [ ] Facebook
- [ ] Twitter
- [ ] Instagram
- [ ] Snapchat
- [ ] LinkedIn
- [ ] Google+
- [ ] Other:

For what purpose(s) did you use your social media(s)? *
(For personal use)

- [ ] Communication
- [ ] Playing Games
- [ ] Watching Videos
- [ ] Online Purchasing
- [ ] Other:

What kind of content do you usually share on your social media(s)? *
(While using it in workplace)

- [ ] Text message
- [ ] Picture
- [ ] Video
- [ ] Voice message
- [ ] Other:

What do you know about information security? *

Have you attend any "Information Security Awareness" training? *

- ◯ Yes
- ◯ No

If yes, where?

Appendix 2: Interview with the Chief Operating Officer of Conclave

Interviewer: Sabrina Soebhektie
Interviewee: Akbar Maulana, Conclave

Topic: Information Security Awareness
Date: 14.10.2015

Questions:

1. What is an information security in your opinion?
   Answer: [redacted]

2. Why do you think information security is important?
   Answer: Mostly because we uses public media to share a lot of information, and we never know what can happen to those information that we shared.

3. Have you had any experience with oversharing?
   Answer: Personally, no. I am not the kind of person that like to share my personal life in social media. Thankfully, I have never seen any employees of Conclave overshared anything work-related in their social media, although they are very active in it. I have seen a lot of people did that (oversharing a work-related information), and it is very shameful to see people that are not educated enough to know the boundaries.

4. Which of the social networking sites do you use?
   Answer: I have accounts for almost every social medias, but I mostly use twitter as my source of current news and articles. Other than that, I usually uses instant messaging type of social media for the obvious reason.

5. What are your expectations from this research?
   Answer: I want our team to be more conscious about the risk of oversharing. Because, social media is a big part of our business, and also our personal life, and it is impossible to not let them use it. Therefore, I want our team to be fully understand about this topic, before something might actually happens.

Appendix 3: Results of Questionnare

Platform	
Facebook	6
LinkedIn	7
Google+	3
Twitter	9
Instagram	5
Snapchat	1
Dropbox	1

Usage	
Communication	9
Data storing	6
Promotion	5

Usage	
Communication	8
Watching Videos	5
Online purchasing	1
Others	4

Type of Content	
Text message	9
Picture	7
Video	3
Others	1

Knowledge	
Yes	1
Nothing	5
Somewhat	3

Training background	
Yes	0
No	9