Master thesis

Factors Related to Users’ Awareness of Information Security on Social Network Service

--The Case of WeChat

Author: Shen Han
Supervisor: Behrooz Golshan
Examiner: Anita Mirijamdotter
Date: Feb, 08, 2018
Subject: Information System
Level: Advanced
Course code: 5IK50E
Abstract

Recent trends in social network services (SNS) have taken the rates of personal information sharing, storage and processing to an unprecedented level, which yield both benefits and undesirable consequences for their users. SNS is being exploited by criminals to fraudulently obtain information from unsuspecting users. User’s awareness of privacy protection has been far left behind by the increasing and popularizing utilization of social network services (SNS), the privacy security problems will become one of the important factors influencing the healthy development of social network service industry.

This study was designed to collect data and produce knowledge about the security awareness of WeChat users (i.e., randomly selected from all over China), their preferences and their experience of using WeChat while facing security issues as well as the perspectives of how people perceive a specific security problems, in order to find out what factors influence user's security awareness. In order to carefully conduct the research process and explain the empirical findings, seven principles of interpretive field research and protection motivation theory is adopted as core theoretical foundation. Participants were asked to provide information about and their personal views of questions from their different experience and value. Eight persons interviewed for our research and their responses confirmed our objectives of the study. As a result, six factors are indentified in related to WeChat user’s security awareness. PMT helps to explain and understand that how six indentified concepts influence behaviour intention and security awareness of user.

Keywords

Social Networking Services, Cybercriminal, Security Awareness, Protection Motivation Theory, Personal Information, Privacy Protection, WeChat, China
Acknowledgements

First of all, I would like to show my appreciation to my thesis supervisor Behrooz Golshan for her constant support. I would like to thank him for his insightful comments. His guidance was valuable for leading me to the right pace. I really thank Behrooz for his support.

Secondly, I would like to sincerely appreciate the examiner Christina Mörtberg for inspiring me and guiding me to the right direction in my master thesis.

Lastly, I would like to thank all the eight participants for their involvement in this study. Without their contribution, the result of study would not be generated successfully for me and my research process.
## Contents

1 Introduction and Motivation .......................................................... 1  
  1.1 Information security awareness in context .................................. 5  
  1.2 Research questions ................................................................. 6  
  1.3 Scope and limitations ............................................................... 7  

2 Theoretical Foundation ............................................................... 9  
  2.1 Current knowledge of the field .................................................. 9  
    2.1.1 Current situation of SNS in China ....................................... 9  
    2.1.2 Access to user’s personal information .................................. 10  
    2.1.3 Information security awareness ......................................... 10  
    2.1.4 SNS user’s security awareness ......................................... 11  
  2.2 Factors related to security awareness ....................................... 12  
  2.3 PMT – Protection Motivation Theory ....................................... 14  

3 Research Methodology ............................................................... 19  
  3.1 Philosophical Assumptions in IS Research .................................. 19  
  3.2 Research Methodology ............................................................ 21  
    3.2.1 Qualitative method ......................................................... 21  
    3.2.2 Seven Principles for Interpretive Field Research .................... 22  
  3.3 Data Collection Technique .................................................... 25  
    3.3.1 Interview ......................................................................... 25  
    3.3.2 Documents Analysis ....................................................... 28  
  3.4 Data Analysis Approach .......................................................... 28  
    3.4.1 Memoing: Producing Evidence through Writing .................... 29  
    3.4.2 The Three Cs: Coding, Categorizing, and Identifying Concepts 29  
  3.5 The Empirical Setting -- WeChat ............................................. 30  
    3.5.1 Features .......................................................................... 31  
    3.5.2 Security concerns ............................................................. 34  
  3.6 The multiple functionalities of WeChat ..................................... 35  
  3.7 Evaluation Criteria of the Research ......................................... 38  
  3.8 Ethical Consideration .............................................................. 39  

4 Data Analysis ................................................................................ 41  
  4.1 The Results of Initial Coding .................................................... 41  
  4.2 Categorizing and Identifying Concepts ..................................... 43  
    4.2.1 Essential Tool .................................................................. 44
1 Introduction and Motivation

The most adverse outcomes of social networking use are breaches of personal information security (Reyns and Henson, 2016). Recent trends in social network services (SNS) have taken the rates of personal information sharing, storage and processing of big data analysis to an unprecedented level (Conger et al., 2012), which yield both benefits and undesirable consequences for their users.

Social network services are being exploited by criminals to fraudulently obtain information from unsuspecting users. Unfortunately, the illusion of safety assumed by most users makes them vulnerable to the potential online dangers (Okesola, Onashoga and Ogunbanwo, 2016). Personal and security sensitive information losses resulting from cybercrime, including online identity theft or usurpation (Reyns and Henson, 2016), financial fraud, stalking and blackmail, are on the rise (Gradon, 2013).

The problem is that user’s awareness of privacy protection has been far left behind by the increasing and popularizing utilization of social network services (SNS), the privacy security problems will become one of the important factors influencing the healthy development of social network service industry (Xu, 2014). Tow at al. (2010) conclude that users are often simply not aware of the issues or feel that the risk to them personally is not dangerous, and have had a naive sense that online communities are safe. People are always posting messages, updating their status, liking other postings and sharing photos and videos on their SNS, which increase the risk of the information breach. Alqubaiti (2016) indicates that what individuals post or share could potentially violate their privacy and security on the Web. The National White Collar Crime Center (NW3C) provides a list of crimes linked to social media including burglary, phishing & social engineering, malware, identity theft, and cyberstalking (National White Collar Crime Center, 2013). According to the National Cyber Security Alliance (NCSA) in 2011, 15% of Americans had never checked their social networking privacy and security settings (National Cyber Security Alliance, 2011). Meanwhile, in China, 2015, only 35.8% of Chinese took the initiative to check the privacy controls of SNS, up to 56.2% of users did not pay attention to the privacy issues of SNS (CNNIC, 2016). Alqubaiti (2016) concludes that it is critical for the users to be aware of the vulnerabilities of SNS and act with caution.

This study mainly focuses on different SNS users in China since the protection of SNS user's personal information in China is facing a significant challenge. In emerging markets, China is one of the most affected countries by cybercrime. According to the CNNIC (China Internet Network Information Center) (2016), In 2015, network security incidents caused economic losses of 91.5 billion Yuan, which is about 12.3 billion Euro. All incidents were attacks on individuals including spam, fraud information, and personal information disclosure (CNNIC, 2016). In this circumstance, user’s personal information are likely to be disclosed. Users' initiative to participate in social
networking has been severely affected, which also affects the healthy development of social networks (Luo, 2012). Luo (2012) emphasized that the lack of security awareness among users is one of important reason for such privacy problem. From previous researches, Hänsch and Benenson (2014) concluded that security awareness means that the users should be aware of which threats, dangers, and risks exists, and the users should also be aware of which kind of measures they can apply to protect themselves. It is about users’ attentions on security and how well they recognize IT security problems and concerns, and how they should respond to that.

This paper consists of two parts. First of all, it make a interpretive analysis of the current situation of SNS user’s security awareness from the view of user’s behavior, and several semi-structured interview are conducted with users of WeChat. Secondly, from the perspective of user’s behavior, the thesis analyze the factors that are affecting the formation of user security awareness in terms of Protection Motivation Theory. The findings of this study will help inform the development of social network user awareness practices in China and the enhancement of security mechanisms implemented on social networking platforms.

Information technology and social networks are increasingly embedded in people's daily life. While the benefits of information communication technology are outstanding, but they also come with risks of privacy issues like data losses, financial losses, damages to reputation, intellectual property theft and legal problem. These security challenges might be more influential than positive impacts to organizations and individuals (Boddy, Boonstra and Kennedy, 2008). Therefore, information security is a signigicant concern for the development of social network services (Njenga and Brown, 2012).

Social network services offer a new range of opportunities for communication and real time exchange of all kinds of information, however, privacy and security have emerged as critical issues in the SNS environment (Donath, 2007). While such failures have frequently been reported in the press, individuals continue to suffer unprecedented privacy breaches. For example, On October, 3rd, 2016, Kim Kardashian was robbed at gunpoint in Paris for millions of dollars worth of jewelry. She had shared a picture of a $4.5 million ring on her Instagram account three days prior. According to a report by Hendricks (2014), in the United States, 81 percent of Internet-initiated crime concerns social networking sites, mainly Facebook and Twitter. One in five adult online users reports that they were the target of cyber crime, while more than a million become victims of cybercrime every day. In emerging markets, China is one of the most affected countries by cybercrime. In 2015, network security incidents caused economic losses of 91.5 billion Yuan, which is about 12.3 billion Euro. All incidents were attacks on individuals including spam, fraud information, and personal information disclosure (CNNIC, 2016). For example, Some criminals provide QR codes and claim users have the chance to when the gifts if they scan the QR codes and follow the official account.
Once the user scans the codes, their personal identity information, the bank card number and even passwords are disclosed to criminals and result in funds stolen. Those QR codes have Trojan virus, and it is hard to identify whether it is a safe link. In this circumstance, user’s personal information are likely to be disclosed. Users' initiative to participate in social networking has been severely affected, which also affects the healthy development of social networks (Luo, 2012).

Therefore, many studies have been conducted on the privacy concern of social media. However, much of the relevant literature dealing with security and privacy is based on studies conducted in corporate environments. These studies emphasize potential economic losses to organizations as a result of online information disclosure (Campbell et al., 2003; Rauch, 2001), but not much focus on the negative aspects of technology at the individual level (Saridakis et al., 2015).

There are several motivations for this thesis. First, the lack of privacy awareness among SNS users has been a significant loophole for information disclosure and cyber crime through SNS (Tow et al., 2010). Earlier researches have shown that people do not have much knowledge about the actual privacy risks in the SNS environment, and they are unaware of the risk of information disclosure (Cranor et al., 2006; Tow at al., 2010).

Second, with the increasing and popularizing utilization of SNS, user’s awareness of privacy protection has been far left behind, this problem is more serious in China. According to the ‘Statistical Report on Internet Development in China’ (CNNIC, 2017) by China Internet Network Information Center, as you can see from the figure, in 2016,
by cyber criminals because of the lack of security awareness. The figure 1.1 shows that users is not aware of being a dangerous social network environment. Under such circumstances, it is necessary to assess the user’s privacy level using SNS, and find out the factors that are affecting the formation of user security awareness.

Third, in China’s market, With the rapid development of mobile Internet, new services have been coming up all the time, so that the user's network environment has been becoming increasingly complicated (CNNIC, 2017). As of December 2016, the scale of Chinese Internet users reached 731 million, a total of 42.99 million new users throughout the year (CNNIC, 2017). The development of mobile Internet is still the primary factor driving the growth of Internet users. Social network as a basic application has entered a period of mature and steady development. Social network services are growing through the expansion of service content, which leads to a more complex environment and increases the risk of information disclosure (CNNIC, 2017). In this huge market, WeChat is the most commonly used SNS among Chinese Internet users, up to 79.6% of total Internet users (CNNIC, 2017).

At the same time, the problem of information security of WeChat should be taken seriously. For example, according to the report by Sina-Finance (2017), in April 2017, Chinese police detected a great case of citizens personal information disclosure. Twenty suspects illegally accessed to all kinds of citizens personal information more than 700 million items, a total of more than 370 Gigabits of data. Two hackers were captured since hacking related information system. Police introduced that a intermediary was trafficking the stolen data as well as other types of data like the pregnancy test, car owners, banks, finance and so on. Moreover, police found that there is a greater gang that traffic personal information behind the intermediary. This is a complete industry chain of selling personal information, the bottom of the buyer is the telecommunications fraud group, the upper buyer is information selling intermediary, and the source is the network hackers. The police who were handling the case reminded that sharing sensitive personal information on WeChat moment would cause leakage as well as using WeChat payment through scanning two-dimensional code. The lack of privacy protection, as well as the misunderstanding of the virtual community may leave the chance for criminals (Li, 2013).

Finally, previous studies emphasize potential economic losses to organizations as a result of online information disclosure (Campbell et al., 2003; Rauch, 2001), and the impact of government censorship (Lien and Cao, 2014; Harwit, 2016), at the same time, not much has been focus on the negative aspects of technology at the individual level (Saridakis et al., 2015) and concerns caused by online criminals and third parties. The notion of self-disclosure of personal information (Jiang et al., 2013) has been central to information system research into the research of privacy online. All of these concepts have been studied widely in online environments. However, privacy and information disclosure have been shown to be dependent on the online context (Nguyen et al., 2012).
and on individual (Xu et al., 2014) and other factors, in the social media contexts – all of which have not been fully understood in IS research. The intention is to contribute with the research to understand factors that affecting the privacy awareness of SNS users in more detail.

1.1 Information security awareness in context
Most of previous studies elaborate and explain the information security awareness of end-users under the context of the organization rather than the context of individual. Siponen (2000) explained the term "information security awareness" as a state where users in an organization are aware of their security mission. Siponen also emphasized the importance of information security awareness, as information security techniques or procedures can be misinterpreted, misused or not used by end-users, so that losing their real usefulness and effectiveness. Siponen (2000) divided problems related to awareness into two categories including framework and content. The framework category is more a field of "engineering disciplines", comprising issues that can be approached in a structural manner and by quantitative research, that may be formalized and are a matter of explicit knowledge. On the other hand, the content category concern more about the field of informal interdisciplinary, a "non-engineering area", includes tacit knowledge as well, and should be approached through qualitative research methods. And almost all methods regarding increasing awareness have focused on the framework category, but Siponen (2000) believed that the matter lies in the content category is how manager motivate employees to comply with information security guidelines. This research presented the behavioural framework and analyzed current approaches to awareness from the point of view of behavioural theories.

Kruger and Kearney (2006) indicated that information security focuses on protecting the confidentiality, integrity, and availability of information, information security awareness takes care of the use of security awareness programs to create and support positive behavior as a critical element in an efficient information security environment. The goal of a security awareness program is to strengthen the awareness of information systems security in recipients mind and alleviate the possible negative effects of a security breach or failure. The Information Security Forum (ISF, 2003) defines information security awareness as the degree or extent to which every member of personnel understands the importance of information security, the levels of information security applicable to the organization, their individual security responsibilities, and acts accordingly.

It is significant to define the three elements of information security since information security awareness is about to support and maintain confidentiality, integrity and availability of the system, which, in turn, protects user's personal information. According to Åhlfeldt and all (2007), Confidentiality relates to data not being accessible or revealed to unauthorized people. Integrity concerns protection against undesired
changes. Availability concerns the expected use of resources within the desired time frame. These three elements are concerned with the development of all information security programs in organizations, such as information security awareness programs.

In the context of social network services (SNS), information security awareness refers to the ability of SNS users identify threats, dangers and risks exist while using it, and how do they respond it accordingly, in order to reduce security incidents effectively. However, much of the previous studies dealing with security and privacy is based on studies conducted in corporate or organizational environments. These studies emphasize potential economic losses to organizations as a result of information disclosure (Campbell et al., 2003; Kruger & Kearney, 2006; Siponen, 2000), which causes to the paucity of coverage of negative aspects of information security issues at the individual level.

Several studies have attempted to determine implications of security concerns and awareness of privacy to users' online practices and behavior (see e.g. Alqubaiti, 2016; Acquisti & Gross, 2006; Gross & Acquisti, 2005; Jiang et al., 2013, etc.). The real security risks are believed to arise when users disclose identifiable information about themselves online to people who they do not know or normally (that is, offline, in real life) would not trust. This is assumed to stem from the user's lack of security awareness (Gross & Acquisti, 2005).

Govani and Pashley (2005) examined student awareness of the security issues and the available protections provided by Facebook. Researchers found that the majority of the students are aware of potential consequences of providing personal information to the whole Internet (such as, the risk of identity theft or stalking), whereas they feel safety enough in providing their personal information. Although they are aware of ways to preventing the visibility of their personal information, they did not take any action to protect the information (Govani & Pashley, 2005). In another study, Tow et al. (2010) concludes that users are often simply not aware of the issues or feel that the risk to them personally is very low, and have had a naive sense that social network services are normally safe.

A plenty of studies found many factors that influence the level of user's security awareness, and a literature review is given in the next chapter about those factors.

1.2 Research questions

In order to successfully achieve the expected results and benefits, this thesis has formulated a research questions that strategically conduct the study.

In recent years, some researchers have argued that in an Internet environment, information privacy is no longer under the control of individuals but rests with the organizations that hold the information (Conger et al., 2012). Other researchers have
argued that information privacy protection should be extended to include secondary use, access, control, notice and so on (Xu et al., 2014). This places emphasis on privacy as a multi-dimensional concept involving many parties, for example the individuals who provide information and the parties that collect the information, such as vendors, data-sharing partners or illegal entities (Conger et al., 2012), and also highlights the importance of different degrees of management and control over personal data. Particularly for emerging technologies, such as social media, it is necessary to refocus the research direction beyond the scope of individual information management (Wright et al., 2008). In this study, only individual user's aspects are examined and analyzed in order to find out the critical factors that affect user's security awareness.

The research question focuses on seeking the most critical factors that affect the security awareness of WeChat users which is conducted by PMT. The research question is theoretically answered by focusing on the existing literature that has examined relevant factors to understand the importance for user's security awareness, after that, the question is empirically answered through verifying identified theory of protection motivation into the empirical setting of WeChat to understand how factors influence user's awareness in the specific case of China. At last, I will discuss in which way the findings can be used for reference and future research. The research questions are formulated as follows:

What factors influence information security awareness of Chinese social media users?

1.3 Scope and limitations

In this study, only individual user's aspects are examined and analyzed to find out the critical factors that affect user's security awareness.

One of the most significant issues and limitations of information security behavioral and awareness research is that the majority of it has been conducted in Western cultures, with occasional studies being conducted in Asia and elsewhere (Crossler et al., 2013). Most of the rest of the world has been neglected. Meanwhile, There are little has been done to examine cross-cultural considerations involved with insider behavior, IT security compliance, hacking, security violations, and so forth. These are particularly important considerations because culture likely has a direct impact on these issues. This thesis has been conducted in the context of Chinese social media environment as well as all interviewee are Chinese who have been using WeChat for many years. From this cultural perspective, the results are limited to Chinese users who grow up with the specific culture different from western social media users, which might result in different behavior and perceived perception toward information security issues. On the contrary, the thesis does not conduct either from the cultural perspective or involving western users (because of not all of the features of WeChat work worldwide) which is
one of limitations of thesis. So that considering cultural influence or comparing western users perspective with the rest of world could be future directions of information security research.

On the other hand, the use of PMT is also limited since it does not reflect all of the cognitive and environmental variables such as the impact of social norms. Individual action is circumscribed within a social context (Anderson and Agarwal, 2010). Over decades, lots of variables and relationships have been considered in the PMT researches. In addition to the four main factors of PMT, the studies have considered a variety of constructs such as fear, worry, barriers, social factors, and socio-demographic variables as reference to the context under investigation.
2 Theoretical Foundation

2.1 Current knowledge of the field

In this part, the author explains some key concepts and problems of this research, and the description of research objectives.

2.1.1 Current situation of SNS in China

Online social network services (SNS) in China, such as Wechat and Weibo, have been exponentially growing in membership in recent years (CNNIC, 2017). An SNS represents a virtual community in which people with different interests can communicate by posting and exchanging information about themselves. SNS provide users with their own platform to create, build and share information about interests and activities (Shin, 2010). Although SNS offer a plenty of new opportunities for communication and real-time exchange of all kinds of information, privacy and security have emerged as significant issues in the SNS environment (Donath, 2007). Personal data about users become publicly available in an unprecedented way and even more severe, including digital pictures, videos and text. So that some concerns continue to grow over security risks, such as the increased threat of identity fraud triggered by the wide visibility of personal data in user profiles and by possible hijacking of information by unauthorized third parties (Dwyer, 2007). Individuals face the increasing risk of privacy issue over how others will use their data once published on the network, but they are not even be aware of the problem.

The lack of related security technology, regulations, policies and user security awareness highlighted the social network security and privacy problems, which has to be considered immediately and carefully (Sun et al., 2011). Information breaches caused by cybercrime bring massive losses to users. In emerging markets, China is one of the most affected countries by cybercrime. In 2014, about 240 million Chinese users became cybercrime victims, with economic losses of up to 700 billion yuan (CNNIC, 2016). In this circumstance, user’s personal information are likely to be disclosed. Users’ initiative to participate in social networking has been severely affected, which also affects the healthy development of social networks (Luo, 2012).

One of the most popular SNS in China, WeChat, is a prevalent SNS with the features of real-time communication either text, online call or video call; Social networking, users can post or share information about themselves or content they interested from another source; Platformization, WeChat’s platform allows third-party developers to author and market applications to WeChat’s users. Wechat has 768 million active users, it is more than double the entire population of the United States and made over 100 million voice and video calls everyday via the application in 2016. WeChat’s developer -- Tencent Group Holdings Ltd said in a report (Tencent, 2016 a). This SNS application is my research objective, because WeChat is the most representative one with highest market
share among China market, as well as each users spend a lot of time for using it. Therefore, WeChat is also an huge place for cyber crime. Researchers need to do an analysis of user information security awareness about wechat.

2.1.2 Access to user’s personal information

There is an important question need to consider when dealing with privacy risk -- who has access to users' personal information shared on the SNS. Before discussing this question, the definition of personal identifying information (PII) needs to be clarified. Kosta and Dumortier (2008) highlight that PII is any kinds of information which can potentially be used to uniquely identify, contact, or locate a single person. Understanding the concept of PII has become much more important because information technology and the Internet has made it easier to collect that information.

According to Gross and Acquisti (2005), three groups of stockholders was identified which could access user's personal information in an SNS: the hosting service, the network, and third parties. In this research, I mainly focus on third parties access such as a malicious attack from other individual or criminal groups. Because ordinary people are almost hard to avoid data disclose from company or government use. So it’s urgent for users to be aware of security and privacy issues, in order to eliminate possible harms as possible from third party attack. Users may not capable enough to against big internet company or government, but it’s possible to reduce risk by not doing risky actions.

Third parties can access user's information without the help from SNS holders (Gross & Acquisti, 2005). The easiness to join and extend one's network, and the lack of security awareness in most networking sites makes it easy also to malicious third parties, such as identity thieves, which may cause financial or reputation losses. In the case of WeChat, third parties with permission, that is, third party application providers, have a right to access users' data when a user adds their application. Some strangers may use location function to find users nearby (only if the user open the location function as well).

When personal information is accessed by malicious third parties, additional risks associated with privacy become more serious. The nature of the risk depends on the type and the quantity of information that has been provided: the information may be extensive and very intimate. These online privacy risks range from identity theft to both online and physical stalking; and from embarrassment to price discrimination and blackmailing (Gross & Acquisti, 2005).

2.1.3 Information security awareness

Hänsch and Benenson (2014) listed three different meanings of information security awareness from previous studies. The Three meanings are:

- Security awareness as perception
- Security awareness as protection
Security awareness as behaviour

Security awareness as perception focuses on the fact that users should know that threats, dangers and risks exist, which is closely connected to the general definition of awareness. Security awareness as perception also relates to the degree an end user thinks something is secure or not (Huang, Rau, & Salvendy, 2010).

Security awareness as protection includes the views of previous studies which demand that the users should be aware of which threats, dangers, and risks exists, and the users should also be aware of which kind of measures they can apply to protect themselves. This meaning of security awareness is about users’ attentions on security and how well they identify IT security problems and concerns, and how they should respond (Hänsch & Benenson, 2014).

Security awareness as behaviour means that the main reasons of information security awareness is to reduce security incidents effectively (Hänsch & Benenson, 2014). This is reached when users know which kind of security measures they can use to protect themselves and how to deploy and maintain software applications. This meaning of security awareness focuses on how users act and think regarding information security, and the degree of which you can transfer knowledge of different factors in information security that may influence the way a user acts or behave (Hänsch & Benenson, 2014).

In this specific case, the definition of security awareness is that how well the WeChat users identify threats, dangers and risks exist while using it, and how do they respond it accordingly, in order to reduce security incidents effectively. It focuses on how WeChat users act and think regarding information security by applying security measures they can use to protect themselves and deploying and maintaining the SNS application.

2.1.4 SNS user’s security awareness

Previous research has shown that people have little knowledge about the actual privacy risks in the online environment, and they are unaware of the volume of personally identifiable information they have provided to an indefinite number of individual or group (see e.g. Cranor et al., 2006; Tow at al., 2010). Cross and Acquisti (2005) also indicate that users may have the relaxed attitude towards (or lack of interest in) personal privacy and myopic evaluation of the associated privacy risks.

Some other previous studies have shown that users normally do not put effort to read the online social services privacy policies and the terms of use (see e.g. Acquisti & Gross, 2006; Luo, 2012; Li, 2013). This phenomenon has been existing both in western SNS and Chinese SNS. Cranor et al. (2006) noticed that users find learning about privacy and reading the privacy policies to be tedious and time-consuming. Some
studies also found that quite many users are aware of privacy features and know how to use them, but they do not take actions to protect their information (see e.g. Acquisti & Gross, 2006; Luo, 2012; Li, 2013). For example, Acquisti and Gross (2006) show in their study that the majority of Facebook users claim to know about ways of managing the visibility and searchability of their profiles, but only a significant minority are unaware of those tools and options.

Compare to Facebook, Wechat focuses more on connecting users to shopping, traveling and other life service needs as the main direction of development (CNNIC, 2017). Which increase the risk of information disclosure as more connection are built between users and third parties, and the whole environment becomes more complex. WeChat is quite different with Facebook or any other western SNS, and there are not much studies are conducted to understand security awareness of WeChat from user’s perspective. So that the gap is clear here.

### 2.2 Factors related to security awareness

A number of previous studies have found and exemplified factors related to user awareness from both organizational and individual perspective. According to Mekovec and Vrček (2011), they proposed a research model that investigate the relationship of various privacy factors and Internet users’ privacy perceptions, which factors are organized in five groups including user-intrinsic characteristics; situation factors; web site characteristics; user and web site relationship; legislation and government privacy protection. The meaning of user-intrinsic characteristics is obvious, which includes education level, Internet literacy, age, gender and any other user’s characteristics that could somehow bring impact on the security awareness. Situation factors are connected to the fact that an individual can react differently in the same situation but under different conditions. For example, user usually would not have same reaction on same security threats with past experiences in a specific situation (Mekovec and Vrček, 2011). The web site characteristics can not be ignored while considering users’ online security awareness. Because strong company’s reputation positively influences users’ trust towards information sharing (Mekovec and Vrček, 2011). User and web site relationship are generally related to individual’s perception and attitudes to information collection during online activity. Legislation and government protection includes factors referring to user's perception of how government and legislation protect their online privacy (Mekovec and Vrček, 2011).

Posey et al. (2010) found that social influence, privacy risk belief, and online trust affect user's privacy awareness. Social influence is the degree to which an individual’s beliefs, attitudes and behaviors are influenced by others in his or her environment (Deutsch & Gerard, 1955). Bandura’s (1977) social learning theory emphasize that individuals’ behaviors are learned responses from the behaviors of other individuals within the
environment. Recently, trust has taken center stage as a serious issue in SNS. Trust is one of the most important factors that affect security and privacy in social networking (Shin, 2010). The higher the user’s trust in the service, the less effort they will exert to scrutinize details of the content. So that trust factor is definitely taken into account in the research for assessing the user’s security awareness. Research studies on social networks have identified that user perceptions of self-anonymity reduce individuals’ privacy concerns which affects privacy awareness (Jiang et al., 2013).

Lebek et al. (2014) provide an overview of theories used in the field of information systems (IS) security behavior of employees over the past decade. The paper identified 54 used theories, and four behavioral theories were primarily used: Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM). Their study shows an overview of determinants that have been proven to influence employees’ behavioral intention. This is valuable for practitioners in the process of designing Security Education, Training and Awareness (SETA) programs, but also enlightening for my research design. Thus, Protection Motivation Theory (PMT) has been selected as the core theoretical foundation of my study. Further use is elaborated in section 2.3. Due to the significance of aforesaid four behavioral theories and they have been widely used in the field of information security research, it is important to make a brief explanation.

Theory of reasoned action/theory of planned behavior (TRA/TPB): In the context of information security behavioral compliance, the employee’s intention to comply with information security policies (ISPs) depends on his/her overall evaluation of and normative beliefs toward compliance-related behavior. The greater the feeling of reflected actual control over those actions, the greater the intention to comply with ISP (Bulgurcu et al., 2010; Lebek et al., 2014).

General deterrence theory (GDT): Adapted from criminal justice research, GDT is based on rational decision-making. GDT states that perceived severity of sanctions (PSOS) and perceived certainty of sanctions (PCOS) or punishment influence employees’ decision regarding ISP compliance by balancing the cost and benefits (Bulgurcu et al., 2010).

Protection motivation theory (PMT): Maddux and Rogers (1983) argue that an employee’s attitude toward information security is shaped by the evaluation of two cognitive-mediated appraisals: threat appraisal (TA) and coping appraisal (CA). An employee who is aware of potential security risks forms attitudes towards perceptions of these threats and the coping response (Anderson and Agarwal, 2010; Herath and Rao, 2009).
Technology acceptance model (TAM): In the security awareness context, the TAM determines the employees’ intention to comply with ISP, which is influenced by perceived usefulness (PU) and perceived ease-of-use (PEOU) of information security measures (Lebek et al., 2014). All four theories explain employees’ behavioral intention (BI) or actual behavior (AB) by adapting different factors. Each behavioral factor has been tested and evaluated in multiple studies. As a result, Lebek et al. (2014) emphasized that qualitative studies like action research and interview studies could add value to the research field due to the dominance of quantitative work. So that, in this study, PMT is applied as core theoretical foundation that help to understand the critical factors towards security awareness of WeChat users and their relationships.

2.3 PMT – Protection Motivation Theory

Protection motivation theory (PMT) has formed the basis for prior security research (e.g., Anderson and Agarwal, 2010; Axelrod & Newton, 1991; Herath and Rao, 2009; Woon et al. 2005) and provides the core foundation for this study. PMT, proposed by Rogers (1975), was originally based on expectancy-value theories and identified the cognitive processes an individual experience when faced with a threat. The original PMT (Maddux and Rogers, 1983) identifies that the motivation to protect depends upon four factors: (1) perceived severity of a threat; (2) perceived vulnerability; and (3) the efficacy of the recommended preventive behavior (the perceived response efficacy). Later, Maddux and Rogers (1983) revised the theory to include perceived self-efficacy (i.e., the level of confidence in one’s ability to undertake the recommended precautionary behavior) as a factor in the coping appraisal process. The intrinsic and extrinsic rewards of risky behavior, as well as the response cost of protective behavior were also included in the model.

Protection motivation deriving from the appraisal of the two processes including threat appraisal and coping appraisal, which is defined as ‘an intervening variable that has the typical characteristics of a motive: it arouses, sustains and directs activity’ (Rogers, 1975, p. 98). Threat appraisal refers to person’s evaluation of the degree of danger posed by the threat. It comprises of perceived vulnerability, perceived severity, and rewards. Perceived vulnerability refers to the person’s evaluation of the probability of the threaten (Maddux and Rogers, 1983). In this study, threat refers to unauthorized access (third party links or apps) or unsafe operation by user to the user’s personal information. Many studies (Rippetoe and Rogers, 1987; Wurtele, 1988) have shown a significant main effect of perceived vulnerability on coping response, with people who shows high levels also showing increased intention to adopt a recommended coping response. So that the perceived vulnerability will be examined whether it has a significant effect on WeChat user’s intention of safer practicing.
Perceived severity refers to the severity of the consequences of an occurrence (Maddux and Rogers, 1983). In this context, loss of personal information and online identity are considered as possible consequences. Previous health related studies (Maddux and Rogers 1983; Milne et al. 2000) found severity to be the least significant of the four cognitive mediating factors. In addition, best practices in IT security management promote a risk assessment approach to managing security risks (Stoneburner et al. 2002). According to this approach, action to reduce the level of risk should be taken when they (risks) become unacceptably high. In this case, respondents are asked what kind of actions would they take in terms of different threats and how they rate the severity of threats, since risk levels should be increase when the severity of the loss from a threat increases.

Rewards refers to intrinsic and extrinsic rewards of not adopting the recommended coping response (Maddux and Rogers, 1983). For instance, the rewards for continued smoking (i.e., not stopping smoking) are physical pleasure and peer approval (McClendon and Prentice-Dunn, 2001). Regarding the rewards construct, Woon, Tan and Low (2005) find that the person does not derive any intrinsic pleasure nor extrinsic approval for not enabling security actions. Therefore this construct was not included in the model.

Coping appraisal refers to the person’s assessment of his/her ability to cope with the potential damage resulting from the threaten. It consists of self-efficacy, response efficacy, and response cost.

Self-efficacy refers to the person’s confidence in his/her ability to perform the required protective actions (Maddux and Rogers, 1983). The construct is adapted to verify the respondents perceived ability of protecting personal data. In studies based on self-efficacy theory, self-efficacy has been found to have a significant positive correlation on behavioral change (Bandura et al., 1980; Condieotte and Lichtenstein, 1981). In addition, significant correlations between self-efficacy and coping response have also been found in a wide range of PMT related studies (Maddux and Rogers, 1983; Stanley and Maddux, 1986). A quantitative study by Milne et al. (2000) has also shown that among all PMT independent variables, self efficacy has the most strong effect on intention. In this case, the correlation will be examined by qualitative method, to see if social media users have same pattern in China.

Response efficacy refers to the efficacy of the recommended behavior (Maddux and Rogers, 1983). Past quantitative studies (Stanley and Maddux, 1986; Wurtele et al., 1988) have shown positive correlation between response efficacy and coping response ranging from significant to medium effects. In the context of social media, numerous tips or suggestions are given from cyber-security experts, such as customize privacy options, control comments, avoid accidentally sharing personal details, change
password periodically and so on. In this case, the interviewees are asked the actions they perform to protect information. The efficacy of the actions will be discussed.

Response cost refers to the perceived opportunity costs in adopting the recommended action (Maddux and Rogers, 1983). Support for the link between response cost and coping response is given by Neuwirth et al. (2000). Response cost in this case showed as the inconvenience of changing habits of user and the compromise of attractive contents.

The base protection motivation model theorizes that a person assesses a threat based on their own perception of the severity of the threat, vulnerability to the threat, or its probability of occurrence. Once the threat has been evaluated, the person assesses the efficacy of the recommended response to the threat and self-efficacy regarding the protective actions required to mitigate the threat (Anderson and Agarwal, 2010). The major assumptions of protection motivation theory are that the motivation to protect oneself from danger is a positive linear function of four beliefs: (1) the threat is severe, (2) the object is personally vulnerable to the threat, (3) the object has the ability to perform the coping response, (4) the coping response is effective in preventing the threat. In addition, the motivation is a negative linear function of the reinforcements associated with the maladaptive response, and the response costs (Maddux and Rogers, 1983).

![Research Model](image)

**Figure 2.1 Research Model**

The study adapt the research model from the 1983 version of PMT, as you can see in figure 2.1. The use of PMT mainly focus on the person’s intention to adopt a safety behavior of protecting personal information, since the data are collected by interviews which could only obtain a person’s intention or willingness about taking action rather than actual behavior. I consider mainly intention and take it as a variable distinguishing between WeChat users who are going to enable security actions and those who are not. Regarding the rewards construct, Woon, Tan and Low (2005) find that the person does not derive any intrinsic pleasure nor extrinsic approval for not enabling security actions. Therefore this construct was not included in the model.
PMT has been primarily applied in health and environmental settings to investigate which advertising messages effectively motivate a person to take action when faced with a threat (for examples in health-related anti-smoking studies). The information security issue, to be more specific, cybersecurity issue is similar to select health and environmental concerns in that every individual can make a difference. Securing cyberspace is defined in "National Strategy to Secure Cyberspace" (DHS, 2003) as preserving the healthy functioning of the infrastructure that supports critical work. Partially, it depends on every Internet users doing his/her share to ensure security. Therefore, individuals must not only believe that individual action is essential in the fight to secure cyberspace, but they must also further perceive that individual effort makes a difference in the security and privacy of personal information.

PMT has been used in a variety of fields (Floyd et al., 2000; Milne et al., 2000; Herath and Rao, 2009). Primarily related to threats presented to an individual. For instance, in a meta-analysis conducted by Floyd et al. (2000), PMT is one of the most powerful theories predicting individual intentions to take protective behaviors. In the context of information security, Anderson and Agarwal (2010) tried to discover the understanding of what drives home computer users to behave securely online, and the insights into how to influence their behavior by applying PMT as the significant foundation. Although they evaluate intentions rather than behavior because difficulties of observing actual security behavior, but the relationship between behavioral intention (BI) and actual behavior (AB) has been shown to be tight and consistent, as well as theoretically grounded (Anderson and Agarwal, 2010; Lebek et al., 2014). So that behavior is substantively assessed by technically measuring intention (Anderson and Agarwal, 2010). Bulgurcu et al. (2010) argue that an employee’s attitude toward information security is shaped by the evaluation of two cognitive-mediated appraisals: threat appraisal (TA) and coping appraisal (CA). An employee who is aware of potential security risks forms attitudes towards perceptions of these threats and the coping response (Anderson and Agarwal, 2010; Herath and Rao, 2009).

PMT also has been used to understand the individuals’ behaviors based on their perception of threats posed to themselves and their environment. For example, in the case of nuclear threats, the threats are not only posed to the individuals but also to the society surrounding the individuals (Axelrod & Newton, 1991). In the context of information security, if the organization is affected by a threat, an employee within that organization is likely to feel some effects (Herath and Rao, 2009). Thus, the concepts explored in the PMT and fear appeal literature can be applied to and are relevant in the context of information security. In the information security literature, in addition to threats affecting individuals (Anderson and Agarwal, 2010), PMT has been applied to threats posed to organizations in a security policy compliance context (Herath and Rao, 2009). In this case, although the individual user’s behavior in a social media
environment may not directly suggest a concern for social pressure, but some aspects of social influence are relevant, like spreading threats to others without awareness.

In this case, PMT is applied to examine the most critical factors that affect the security awareness of WeChat users because individuals may perceive different levels of threat toward the personal information they intend to protect. An individual who is aware of potential security risks towards his/her personal information forms attitudes towards perceptions of these threats and the coping response. The aforementioned assumptions of PMT yield six sufficient conditions that are prerequisite to eliciting protection motivation and coping behavior, which contains: An individual must believe that (1) the threat is severe; (2) he or she is vulnerable; (3) he or she can perform the coping response; (4) the coping response is effective; (5) the rewards associated with the maladaptive response are outweighed by the factors decreasing the probability of making the maladaptive response; (6) the costs of the adaptive response are outweighed by the factors increasing the probability of making the adaptive response (Maddux and Rogers, 1983). During data analysis phase, the six conditions are used to help me to understand the meanings and intentions of the WeChat users being studied. I try to understand what affects individual WeChat users to behave carefully or not, and the insights of what factors influence user's security awareness as well as behavior by practicing PMT as the core theoretical foundation.

There are weaknesses to this theory since it does not reflect all of the cognitive and environmental variables such as the impact of social norms. Individual action is circumscribed within a social context (Anderson and Agarwal, 2010). Tanner et al. (1991) revised PMT to incorporate the impact of social norms and prior experience on the protection motivation process. For example, young people may believe smoking is harmful to their health but may smoke because of social pressure to be accepted. Also, Tanner et al. (1991) incorporate an individual's prior experience, which contributes to perceptions about costs and benefits associated with actions, as influencing behavior (Anderson and Agarwal, 2010; Bulgurcu et al., 2010; Herath and Rao, 2009). Over decades, lots of variables and relationships have been considered in the PMT researches. In addition to the four main factors of PMT, the studies have considered a variety of constructs such as fear, worry, barriers, social factors, and socio-demographic variables as reference to the context under investigation.
3 Research Methodology
3.1 Philosophical Assumptions in IS Research

In this case, the interpretivism is selected as the philosophical assumption of the research since the research focuses on the user's perspectives, experiences, beliefs, and interpretations that they perceived while using WeChat. So that positivism and critical perspectives are not eligible for this purpose as the research methods and tools of the natural sciences are seen as being inappropriate for the study of social and organizational phenomena (Myers, 2003).

In Information Systems research, there are three philosophical assumptions, the interpretivism, positivism and the critical perspective. These assumptions determine how to study and understand the under examined phenomenon, how to seek answers for them and how to analyze and interpret the data, and then produce the results, as they have different ontological and epistemological background (Myers, 2003; Orlikowski and Baroudi, 1991). According to Orlikowski and Baroudi, (1991) in a broader perspective, the meaning of ontology refers to explain what constitutes reality, as this reality is composed by objectivism or subjectivism and probably depends on individuals and their personal beliefs regarding an issue. Subsequently, epistemology refers to the meaning of knowledge and how this knowledge should be acquired. These three paradigms (interpretivism, positivism and critical) follow a different kind of perspective regarding their ontological and epistemological background.

In the perspective of positivism, the reality is objectively given, independent of the observer and his instrument while relied on quantitative data. Lincoln and Guba (1985) indicate that the positivism assumes that the phenomenon of interest is single, and there is a unique description of any selected aspect of the whole phenomenon. The Critical perspective implies that reality is produced and reproduced by people as it focuses on oppositions and contradictions because people be able to change social and economic circumstances. Moreover, according to Orlikowski and Baroudi, (1991) the critical paradigm related to the creation of awareness to make more comprehensible the multiple forms of the social domination, thus, people can take action and eliminate them.

Positivistic paradigm is not used in this thesis since the study relies more on qualitative rather than quantitative data. And also, the study does not apply the critical paradigm since the main goal is not to arise the inequalities amongst the under examined phenomenon as an emancipator, but to explore the different worldviews that the participants perceive and explain and after that to establish suggestions for improving the problematic field.
On the contrary, according to Orlikowski and Baroudi, (1991), the interpretivism concern with the effort to understand phenomena via the meaning that people assign to them as the world and reality is socially constructed. The interpretative approach attempts to understand a unique person’s worldview. Producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context. It focuses on the full complexity of human sense making as the situation emerges. In this case, the interpretive paradigm is adopted for producing a deeper understanding of the problematic field which is to identify possible factors that are influencing the construction of WeChat user's security awareness (Myers, 2003).

For this purpose, the research focuses on the user's perspectives, experiences, beliefs, and interpretations that they perceived while using WeChat. Their perspectives, experiences, beliefs, and interpretations will support to build a better knowledge on what factors would bring significant impact to the construction of user's security awareness. Orlikowski and Baroudi, (1991) and Walsham (2006) referred that interpretative researchers relied on the subjective experiences of the social actors which make sense of the world. Also, for Klein and Myers (1999) the interpretative paradigm in information systems research help researchers to deeply understand the human actions under an organizational context while achieving to get an insight into the potential information system development.

In addition, Myers (2003) emphasizes that the importance of context. He indicates that interpretive research tend to focus on meaning in context. They aim to understand the context of a phenomenon, since the context is what defines the situation and makes it what it is. In the context of this research, the social media environment in China is distinct with western countries. Popular social platforms world wide like Facebook, Twitter, Instagram and Youtube are banned by government for some reason, and citizens have a bunch of native social media equivalent with western one. From macro view, variables are differential such as effect of regulation. From micro perspective, the specific function of social media can be different. For example, China is transferring to cashless society by adapting e-payment methods like Alipay and WeChat pay, which may rise security problem of social platform in China. On the contrary, Western world achieving cashless society mainly by credit card and dedicated third-party payment providers like Pay-Pal and Swish. The key point here is that the mindset of Chinese User might be different under specific environment and culture. The meaning of a social phenomenon depends upon its context, the context being the socially constructed reality of the people being studied. For this reason, an interpretive research is needed to understand the meaning of a particular word made by WeChat user in China depends upon its context.
3.2 Research Methodology
3.2.1 Qualitative method

The qualitative method is adopted in this case since the research tries to identify the possible factors that influence the construction of user's security awareness by analyzing verbal and textual data in order to develop the reason of security failure from user's perspective and imply for both information system and users. Qualitative method is fully appropriate for this purpose.

Myers (2003) referred that there are two kinds of research methods include qualitative and quantitative while the researcher chooses one of these two distinctions based on the philosophical assumptions they rely on. According to Myers and Avison (2002), each adoption of these research paradigms will determine how the research will be conducted and therefore evaluated as regards the response of the submitted research questions. At one level, quantitative and qualitative refers to distinctions about the nature of knowledge: how one understands the world and the ultimate purpose of the research. On another level of discourse, the terms refer to research methods - how data are collected and analyzed - and the types of generalizations and representations derived from the data (McMillan & Schumacher, 2006, p. 12).

Doing quantitative studies require the researchers to deal with a large amount of data that need to be analyzed via the usage of statistical tools to extract a general point of view for the examined phenomenon. This kind of approach is more fit in with the positivistic paradigm since it is trying to seek out an objectivistic knowledge that can be analyzed with statistical analyses.

On the contrary, doing qualitative approach requires the researcher to analyze participants’ subjective perspectives and brings personal values into the study. But a quantitative research is more about testing theories, measuring and observing information in a numerically way (Creswell, 2013). According to Myers (2003), qualitative research methods are designed to help researchers understand people and what they say and do. They are designed to help researchers understand the social and cultural contexts within people live. The purpose of qualitative study perfectly fit with interpretive research. A researcher should follow the guideline of the qualitative study when trying to study social and cultural phenomena that are complicated and unmeasurable (Myers and Avison, 2002, p.4). Qualitative research methods take advantage of the utility for understanding the meaning and the context of the research field, and the particular events and processes that make up this phenomenon in real-life settings (Maxwell, 1996).

In addition, one of the primary motivations for doing qualitative research comes from the reality that talking ability is one thing which distinguishes humans from the natural
world. It is only by talking to people, or reading what they have written, that we can find out what people are thinking, and understanding their thoughts goes a long way towards explaining their actions (Myers, 2003).

The purpose of this study is to get a better understanding and interpret users’ subjective beliefs and perceptions of security awareness regarding the WeChat using in China, and how the user's perceived judgment affected by this specific application (information system), also the other way around. Based on this purpose, the qualitative approach is adopted in this case since qualitative research is the best way to understand people’s motivations, their reasons, their actions, and the context for their beliefs and actions in an in-depth way (Myers, 2003). This study try to identify the possible factors that influence the construction of user's security awareness by analyzing verbal and textual data in order to develop the reason of security failure from user's perspective and imply for both information system and users.

3.2.2 Seven Principles for Interpretive Field Research

In this case, the research is a basic interpretive qualitative study (Merriam, 2002). The goal of the research is to understand how participants make meaning of a situation or a phenomenon. Therefore, the researcher serves as the filter for the meaning, using inductive strategies with a descriptive outcome. In order to effectively evaluate the research process, Klein and Myers’s (1999) seven principles for the evaluation of interpretive research in information systems are adopted.

Klein and Myers and (1999) proposed seven principles for the evaluation of interpretive research in information systems. Seven principles are (1) The fundamental principle of the hermeneutic circle; (2) The principle of contextualization; (3) The principle of interaction between the researchers and the subjects; (4) The principle of abstraction and generalization; (5) The principle of dialogical reasoning; (6) The principle of multiple interpretations; (7) The principle of suspicion. They also emphasized that the principles are helpful because they summarize important insights in interpretivism which are not embedded in the practice of interpretive field research. Some principles are adapted by this study to conduct and evaluation of interpretive research. In this section, I will be deciding how and which of the principles are applied and appropriated in this matter.

First of all, the fundamental principle of the hermeneutic circle is foundational to all interpretive research as well as to all the other principles. It suggests that all human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form (Klein and Myers, 1999). In this case, the parts are the interpretive researcher and the participants’ preliminary understandings about security problem of WeChat they perceived. The whole is the context of security awareness research in globe, in this study, the context of Protection Motivation Theory. Hence, in a number of iteration of the hermeneutic circle, a complex whole of shared
meanings will emerge, and then, forming a complex web of interpretations between whole and parts.

The principle of contextualization requires the critical reflection of social and historical background of the research setting so that the intended audience can see how the current situation under investigation emerged (Klein and Myers, 1999). In this case, social and historical backgrounds are significant for doing research since the macro and micro environment of social media in China has some differences compare with western country as well as particular culture and conventions towards the security problem investigated. The results of this research might be influenced by the social background and the research itself becomes a part of the society’s future history. In order to reflect the principle of contextualization, this research see participants as the producers of society background and the description of the social and cultural context also reflect the interaction between participant and context.

Thirdly, the principle of interaction between the research and the subjects concern with how the research materials were socially constructed through the interaction between the researcher and participants as well as how researcher’s understanding improved (Klein and Myers, 1999). This principle requires the researcher to place himself/herself and the subjects into a historical perspective. In order to achieve this requirement, interview is adapted for data collection process as well as to interact with the participants back and forth. The research does not relies solely on historical secondary data but first-hand data from participants. As the researcher, I have been using WeChat for many years, and I have a better understanding of the system than others who have not. However, my preconceptions about the object and the participants may affect the construction, documentation, and organization of the material. So I have to embrace the context and participants’ mindset in which I am conducting the research.

According to Klein and Myers (1999), the principle of abstraction and generalization requires relating the idiographic details revealed by the data interpretation through the application of theory one and two to theoretical, general concepts that describe the nature of human understanding and social action. Because the validity of the results and findings drawn from the data not only depend on the data collected but also on the plausibility and cogency of the logical reasoning used in describing the results from the research (Walsham, 2006). In this case, findings are discussed in related to Rogers’s (1975) Protection Motivation Theory. This theory plays a crucial role in the research, and obviously distinguished it from just isolated incidents. According to the PMT, a person assesses a threat based on their own perception of the severity of the threat, vulnerability to the threat, probability of occurrence and its self-efficacy. The theory assumes that the motivation to protect oneself from danger is a positive linear function of four beliefs: (1) the threat is severe, (2) the object is personally vulnerable to the threat, (3) the object has the ability to perform the coping response, (4) the coping
response is effective in preventing the threat. The theory works as an ‘assistant’ to view the data in the certain way.

The principle of dialogical reasoning requires the researcher to confront his/her perconceptions which guided the original research design with the data that emerge through the research process (Klein and Myers, 1999). In this case, the research proposes the general interpretivism with the PMT of Rogers (1975) as integrative frame work for researching the security awareness of information system’s user.

Regarding the principle of multiple interpretations, Klein and Myers (1999) emphasize the researcher to examine the influences that the social context has upon the actions under study by seeking out and socumneting multiple viewpoints along with the reasons for them. The principle is illuminating for doing interpretive research since interpretations of the participants in the field could be various and conflicting related to power, economics, or values. In this case, the biggest confrontation of conflicting interpretations among the participants is what issues should be considered as security problem. The viewpoints by participants could imply how user’s security awareness is constructed under certain circumstances.

The seventh one is the principle of suspicion which is to reveal the effects of socially created distortions and psychopathological delusions (Klein and Myers, 1999). The principle is also applicable to this study since it provides a critical perspective and do not take participants’ views at face value. In this case, the critical perspective is taken by examining the statement of participants in terms of the cultural interests and personal background.

Additionally, the seven principles was followed to conducte and evaluate of interpretive field of research in information system. The principles help me to concentrate on fieldwork and design my investigations more systematically. But it is important to mention that I spent considerable time deriving the theoretical foundations for the research from diverse literature. Even I focused on the seven principles of interpretive field study and qualitative study, since I had to consider each one of the principles systematically and ensures that none has been left out arbitrarily.

In this case, the seven principle should continue until the apparent contradictions and oppositions in the data of interview no longer appear strange, but make sense. Accoding to Myers (2003), from the perspective of a qualitative researcher the fieldwork is not complete until all the apparent contradictions are resolved in the researcher’s mind. The goal of interpretation is ‘to produce a reading of the text that fits all important details into a consistent, coherent message, one that fits coherently into the context’ (Diesing, 1991).
3.3 Data Collection Technique

Qualitative research methods are designed to help researchers understand people and the social and cultural contexts within which they live. The goal of understanding a phenomenon depends on the view of the participants, and its particular social and institutional context is mostly lost when textual data are quantified (Creswell, 2013). This research focuses on qualitative method to use semi-structured interviews and document analysis as the source of data collection. All of the sources will be gathered from the user of WeChat in China.

The selection of participants included the users of WeChat all around China, They are from six different provinces or cities including Liao Ning, He Bei, Gan Su, Shan Xi, Shan Dong and Beijing. The selection of participants aim to collect multiple different experiences and perspectives regarding the information security awareness issues. As the suggestion by supervisor Behrooz Golshan, no researcher’s friends or acquaintances are selected, so that I published information in another Chinese social media for seeking participants from different areas who has different background. They were totally eight participants. However, I took into serious consideration the possibility to increase the number of participants if no new useful data came up.

Something need to be mentioned here, although the WeChat app could be download and used all around world, it has the English version as well, but researcher decided to distribute the interview guide and the native language of all the participants, the Chinese one. Because the research focus on the Chinese market and user’s only since all WeChat’s functions work 100% under China’s internet environment, which makes the case specific. Additional, the fact is that all participants were from China as they also stated that they could express their beliefs in a better way, in the Chinese language. For the purpose of the study, the consent form and the interview guideline in the English and Chinese language are attached on the Appendix A and B.

During the process of interview and analysis, some participants were contacted multiple times if some new thoughts or ideas occurred. According to Klein and Myers (1999) the interpretive strategy is based on repeated field contacts and allows returning to the field to collect more data and to adapt data collection to the needs and questions resulting from the analysis of the data. The formal interviews rely on an interview schedule for all interviewees, but they are also free to re-contacts afterward in anytime by instant messeging.

3.3.1 Interview

In this case, the interviews remain semi-structured in a conversational pattern, which gives the researcher the opportunity to add important insights as they arise during the course of the conversation, while the previously prepared questions provide some focus as well. It would interpret that from what way SNS affect the user's security awareness
and what critical factors influence the formulation of such awareness. For comprehensive and valuable information, eight interviewees are selected for different region of China who uses WeChat. The researcher will contact with them on WeChat video calling. According to Flick (2014, pp.237), interviews should be recorded and transcribed so that there is a solid database for the analysis. Among the interviews, the researcher recorded audios and take notes for analyzing and gathering information.

The selection of the semi-structured interviews related with the mindset that they are more flexible than the structured interviews while at the same time achieve to extract the unique aspects of the participants (Qu and Dumay, 2011). Subsequently, semi-structured interviews are sufficiently structured not only to highlight specific dimensions of the research questions but also to leave space for each participant bringing new meanings to the topic of the study (Galletta, 2013). Back to the case of this study, the problematic situation arise in an internet-based system of social media which shows significant impact to its users in the internet world of China. However, it is expected that the various worldviews, knowledge and experiences of the users will bring the potential understanding to the security problem of the under-examined social media system.

The interview guide mentions factors may have impact on user’s security awareness forming in term of PMT, and few illuminating questions (see Appendix B). Each of these is introduced by an open question and ended by a illuminating question. Open questions may be answered on the basis of the knowledge that the interviewee has immediately at hand. In the interview, the relations formulated in these questions serve the purpose of making the interviewees’ implicit knowledge more explicit (Flick, 2014, pp.218). A goal of interviews in general is to reveal existing knowledge in a way that can be expressed in the form of answers and so become accessible to interpretation (Flick, 2014, pp.222).

Meanwhile, online interview technique applied in this case, because the target group are mostly in China and both functions work successfully only in China, for instance, WeChat pay has populized all over the country but only works in few scenario outside the country. And also, the interviewees are spread across the country, this can be more difficult to organize and to finance. So that, for validation and comprehensive of data collection, all interviews are conducted via WeChat video calling. Online interviewing is a way to transfer face-to-face interviewing to Internet research. There is a much greater amount of anonymity for the participants, which may protect them from any detection of their person during the research, which can be an advantage (Flick, 2014, pp.236).

Regarding the selection of participants, eight people were chosen from multiple cities of China as participants of interview. Eight participants are from seven different and
pivotal provinces or regions of China, which cover a large portion of the country (mainly north part of China), and able to represent the whole circumstance. However, the samples would be more representative if people from southern China and countryside could be chosen.

For the interview process, all the selected participants were conducted face to face via WeChat video call. The duration of each interview on participant was about minimum forty-five minutes to maximum one hour for each one of the participants. However, it needs to be mentioned that in many cases the interviewees expressed the aspiration to continue the interview process for more than the predefined time due to having interest in the topic. For the privacy of participants, they are named as number in table 1. Province of origin of participants also included in the table after their permission.

<table>
<thead>
<tr>
<th>Participant</th>
<th>Province of Origin</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Liao Ning, China</td>
<td>45 min</td>
</tr>
<tr>
<td>P2</td>
<td>He Nan, China</td>
<td>45 min</td>
</tr>
<tr>
<td>P3</td>
<td>Gan Su, China</td>
<td>50 min</td>
</tr>
<tr>
<td>P4</td>
<td>Shan Xi, China</td>
<td>45 min</td>
</tr>
<tr>
<td>P5</td>
<td>Shan Dong, China</td>
<td>45 min</td>
</tr>
<tr>
<td>P6</td>
<td>He Bei, China</td>
<td>1 hour</td>
</tr>
<tr>
<td>P7</td>
<td>Beijing, China</td>
<td>45 min</td>
</tr>
<tr>
<td>P8</td>
<td>Beijing, China</td>
<td>1 hour</td>
</tr>
</tbody>
</table>

Table 1. Interview Characteristics

Each interview session started with a short informal conversation with each participant about their current status, educational background, general view towards WeChat and so on, in order to feel more comfortable, while at the same time, breaking the ice among us for the upcoming interview. After that, the interview process started with a presentation of the aim of the study and how important participants are for the research. Each participant had also already read the interview guide and the terms of the consent form before the process started. Moreover, I reminded to them that they could withdraw any time they want from the interview process or to refuse to answer in questions that probably made them to feel uncomfortable, a statement that is also included into the consent form. Under participants’ permission, each interview recorded in order to encapsulate as much information is needed for ensuring a deep analysis of the outcomes. While trying to ensure the confidentiality of their beliefs and worldviews, the consent form was signed both by me as facilitator and by the participants as well. Each participant kept one copy of the signed consent form.
3.3.2 Documents Analysis
Documents and their analysis used as a complementary strategy to interviews method, so that the research is also rely on how the reality under study is documented in these kinds of data. Documents such as emails, blogs, web pages, corporate records, newspapers, and photographs record what someone said or what happened regard to issues under investigate. Those data provide some evidence that may allow me to build a richer picture than could be obtained by interviews and fieldwork alone (Myers, 2003). This technique is significant for this study because qualitative research of information system security awareness are mostly conducted under western countries and environment. More information are needed with regard to security issue of WeChat and Chinese environment, which could be obtained by such documents. For instance, online criminal or security report associated with WeChat from press or official government channel.

However, Prior (2011) stated that documents can serve as more than just a record of someone’s actions or thoughts, but the actors in some situation. In other words, the documents can be as significant as statement in social action. For example, a person’s statement of security problem he/she experience can be applied if it is proven to be reliable. In order to assess the quality of documents, Scott (1990, p.6) proposes four criteria for assessing the quality of documents. These criteria are authenticity, credibility, representativeness, and meaning. Payne and Payne (2004) comment on these four criteria as follows:

Authenticity (Is the evidence genuine and of unquestionable origin?) means that the object is what it claims it is; Credibility (Is the evidence free from error and distortion?) refers to how far the author is to be believed (Which way he/she acquired the information?); Representativeness (Is the evidence typical of its kind, and, if not, is the extent of its untypicality known?) refers to the extent to which a sub sample can be taken as representative of a wider set of documents; And the meaning (Is the evidence clear and comprehensible?) refers to how the document should be interpreted and understood (Payne & Payne, 2004). In this case, the four criteria are adapted to assess the quality of documents and decide whether the document is reliable or not.

3.4 Data Analysis Approach

Qualitative data analysis is to transform the data into something that is meaningful to the research and intented audience (Myers, 2003). The point is to come up with some insights that help the researcher and others to understand the WeChat users cognitive process toward security problem and examine what influence their security awareness in terms of PMT. According to Myers (2003), the two main things to watch out for are to make sure that the data I have gathered support the use of the particular data analysis approaches and that the approaches are used in a reasonably consisten manner.
In this case, data are collected from both interviews and documents associated with research subject, which appear to be text or text-analogue. Therefore, Memoing and The Three Cs approaches are adopted in this phase.

3.4.1 Memoing: Producing Evidence through Writing

Memoing are a useful way of starting to analyse the data. Memo writing should not be treated simply as the step of analyzing the data, but it conceptualize the data in narrative form (Lempert, 2007, pp. 245). Esterberg (2002) states that there are two main types of memos: procedural memos and analytic memos. Procedural memos focus on the research process, which summarize what I did and how I did it. Analytic memos focus more on the subject matter. They focus on the data and contain ideas about what the data mean. Memos are written, reread, and rewritten in order to advance to more abstract levels of data (Flick, 2014). They are the first step in developing concepts and themes that arise from the data.

Richardson (1994) distinguishes four categories of notes helpful for documenting and reflecting on the process of research:

- Observation notes to cover perceptions in the field.
- Methodological notes about how methods are applied and how to frame that situation.
- Theoretical notes in the sense of what grounded theory researchers describe as memos.
- Personal notes in the sense of a research diary or journal.

Memoing helped me to make evident how my research advanced and how I develop concepts and themes during analysis.

3.4.2 The Three Cs: Coding, Categorizing, and Identifying Concepts

Lichtman’s (2010) Three Cs approach offer me a guide move from raw data to meaningful concepts (from Coding to Categorizing to Concepts). He broke down this process into six steps.

*Step 1.* Initial coding. Going from the responses to some central idea of the responses.
*Step 2.* Revisiting initial coding.
*Step 3.* Developing an initial list of categories or central ideas.
*Step 4.* Modifying the initial list based on additional rereading.
*Step 5.* Revisiting your categories and sub categories.
*Step 6.* Moving from categories to concepts (themes).
In the first step, the initial coding started with data collection process, it is not too early to begin coding. The initial codes are filtered from interview transcript associate with the central idea of the research.

After a large number of codes are developed, step 2 requires to collapse and rename codes as some of them could be redundant (Lichtman, 2010). In this phase, researcher need to choose whatever works best. The initial codes might be modified based on an calibration of what I have already collected and new raw data.

During step 3, Initial list of categories, initial codes is to organize into categories. For example, certain codes become major topics, and others can be grouped under a major topic and become subsets of that topic.

Step 4, modifying the initial list requires to continue the iterative process. Some of categories may be less important than others, or multiple categories can be combined. The goal is to move from coding initial data through identification of categories to the recognition of important concepts.

Similar with step 2, but in a higher level, revisiting categories suggest that researcher should revisit the list of categories and see whether I can remove redundancies and identify critical elements.

At last, the final step in the process is to identify key concepts that reflect the meaning attach to the data I collect. Lichtman (2010) suggest that fewer well-developed and supported concepts make for a much richer analysis than many loosely framed ideas.

Lichtman (2010) also emphasize that making meaning from qualitative data is a process that moves between questions, data, and meaning. Key points of the process are that it is iterative, circular, and can be entered at any point.

### 3.5 The Empirical Setting -- WeChat

WeChat is a free application that is lunched by Tencent on January 21, 2011, which provides instant messaging services for smart terminals (Baidu Encyclopedia, 2017). WeChat has grown from a voice messaging application into a truly ubiquitous app experience in China. Wechat supports cross-communication operators, cross-operating system platform to quickly send free (need to consume a small amount of network traffic) voice messages, videos, pictures, and text through the Internet, but also can be used to sharing streaming media content and location-based social content. As of the second quarter of 2016, WeChat has covered more than 94% of China's smart phones; monthly active users reached 806 million, users include more than 200 countries, more than 20 languages. Also, the brand's WeChat public account number has more than 8
WeChat is often described as a Swiss army knife super app that seemingly does everything. It allows users to order cabs, buy film tickets, check in for flights, pay bills, listen to music, read news, shop for clothes or meet random people nearby. Despite having an amazing variety of features, the core of WeChat is still messaging. Its primary function is for communication with friends and family.

3.5.1 Features
Some unique WeChat features are different from the ordinary SNS services which need to be mentioned.

- The official accounts platform:
  An open platform through which businesses can access WeChat’s huge user base. For a WeChat user, adding an official account is practically the same as adding a friend. Users can also send messages to official accounts in the same way as their friends. This creates interesting opportunities to use WeChat as a customer service platform. WeChat provides an open platform for businesses to build their own apps on top of WeChat basically ‘apps within an app’ model. Developing for WeChat is much cheaper and easier than native app development for both Android and iOS. The cost of user acquisition is also far lower than with native apps; adding an official account can be done with one click.

Screenshot 1 & 2 – Example of Official accounts and Subscriptions

- Payments:
WeChat Pay has grown extremely rapidly in the past two years. 300 million more Chinese have their bank cards linked with WeChat (Tencent, 2016a). WeChat pay is taken in stores all across in China. In particular, peer to peer micro-payments became extremely popular on WeChat from 2015. Chinese consumers are now comfortable using WeChat for payments. It is now commonly accepted in most stores across China. WeChat Pay sits alongside fierce rival Alipay (Alibaba Group) and China’s default debit & credit card system Union Pay as one of the big three payment options for Chinese consumers. Other players such as Apple Pay, QQ Wallet (also owned by Tencent) and Baidu Wallet hold margin market shares.

- **WeChat wallet:**
  WeChat has strategically partnered with several businesses (e.g. JingDong for E-commerce, Didi for order taxi) to provide an entire range of online stores and services baked directly into the app. The user can use the third party services without skipping to another app, but everything can be done on WeChat and pay by this online wallet service.

  ![Screenshot 3 – Example of Wallet and part of services provided](image)

- **QR codes:**
  WeChat popularized the use of QR codes in China which are now ubiquitous across print media, stores and billboards. Scanning QR codes provide a convenient gateway between the online and offline worlds, but it also increases the risk of cyber crime. For example, some criminals replace offline shop's QR codes physically and provide a fake link. Some users would not be aware of it, which increase the risk of being defrauded.
• WeChat moments:
  An immensely popular feature used to share pictures, links, texts, and videos with friends. Users will scroll through this stream of content in a similar way to the Facebook news feed. The addictive combination of switching between checking moments and chatting with friends provides the core loop. This engages users and keeps them returning to the app.
• Protecting users:

WeChat is a closed and private network which places a high priority on protecting users’ information. The app carefully limits the number of unsolicited messages that businesses can send to their followers. It also does not allow businesses to directly gain access to personal information such as email address or phone number. But information security incidents still cannot be avoided from third party attack on individual users, because of the lack of caution and security awareness for individual users.

![Screenshot 6 – Example of WeChat security tips](image)

These key features make WeChat be successful in China. Some statistics show its success and perch in China, 846 million monthly active users; 10 million more official accounts opened for businesses; 31% of WeChat users make e-commerce purchases through WeChat (Tencent, 2016 a). Estimated monthly payment transactions per WeChat user is 53. In comparison, the estimated number of American Debit and Credit Card holders is 24 and ten respectively (Meeker, 2016).

The key features of WeChat are different with conventional SNS like Facebook or Twitter, which make the case be specific and bring the research about SNS user's security awareness to a new context. Meanwhile, these features increase security and privacy problems to users as well as the risk of information disclosure.

### 3.5.2 Security concerns

Some security concerns are placed in front of stockholders of WeChat. The concerns come from two ways including the threat from government regulation and illegal
activities by internet criminals or third parties. Which is the root reason for this essay, trigger the problem I am investigating at in this case. So that it is important and will be elaborated in this part.

WeChat is a China-based IM under Chinese law, which includes some censorship provisions and interception protocols compare with facebook. WeChat holds the ability to access the text and voice messages and contact books of users and users' location information through the GPS feature (Harwit, 2016). This can be seen as the concern from side of government and mother company—Tencent. But, according to Harwit (2016), Chinese citizens were commonly accustomed to this kind of regulation, and they typically practiced self-censorship in their communications. In small-group WeChat communication among friends or relatives, however, there seemed to be fewer reasons for users to raise issues that were politically controversial. This is also proved by several interviews with Chinese user during the thesis, none of them (8 participants) indicate that they have concern or feel threaten from government and mother-company control. This kind of concern is not a major consideration of this thesis, but the threat of user’s careless behavior and online criminal by third parties.

On the other hand, the security threat users concern most is from third parties and online criminals, which is also proved by interviews, 7 of 8 participants indicate that they would be very careful when they deal with activities associated with third parties like personal information authorization. With regard to WeChat, a small-group oriented application, the limits set by users and by the app’s functions serve to limit the ways that information can be shared and propagated (Harwit, 2016), which reduces users’ visibility and increases privacy. But user's careless behavior and illegal attack make their information vulnerable. But user's careless behavior and illegal attack make their information vulnerable, which is the research objectives and the factors cause that. Those points will be emphasized on the rest of thesis.

3.6 The multiple functionalities of WeChat

In order to collect complete and comprehensive data and information about user security awareness, attitudes and behavior, the researcher get contact with WeChat users in China. There are a plenty of social network services with various additional functions on China's software market. This time, the study only focus on a widely used SNS in China named WeChat.

WeChat’s multiple functionalities are now strongly woven into the fabric of users' daily life. As such, this is now known as the WeChat ecosystem, and it continues to expand into new territories and new aspects of daily life. In this chaper, WeChat’s specific features and capabilities are presented, which makes sense of why the case of WeChat is so special to other similar application in the market.
Basically, WeChat can be used for a plenty of things user wants to do online. Although Tencent company does not own all of the products that reside within its ecosystems, it does facilitate simple integration between most of China’s most popular apps. In WeChat, there are equivalents of Western apps like Seamless, Tinder, and Swish, along with hundreds of other popular services.

Here you have some examples:

**Mobike**
This bike-sharing program enables user to pay for rides using WeChat pay. It is similar to bike-sharing projects in cities worldwide but one difference -- it does not require docking stations.

Bikes can be parked anywhere in major cities, which certainly has created some pick-up points. Mobike is not owned by Tencent, but the functionality resides within the WeChat application.

**Donate Your Step**
This mini app permits users to make small donations to charity by using each 10,000 steps they walk on a daily basis. For each 10,000 steps, a user can donate 1 Yuan, which is equal to roughly 15 cents. There is also a leaderboard, which shows the user how they compete to their friends. All of this encourages people to exercise and donate to charity on an ongoing basis.

**WeChat pay: WeChat’s killer app**
WeChat Pay, as known as WeChat Wallet, it is a user’s digital wallet, and it is used to pay for everything that supports it, either by a tap of the phone or a snap of a QR code. WeChat Pay reaches over 600 million active users, compared with 450 million of its chief rival -- Alipay, owned by Alibaba. Alibaba was the market leader until 2014 since the seamless property of WeChat’s integrations has led it to take a sizeable lead. WeChat Pay has many options. The user can send and receive gifts, pay their rent, or donate to a wide variety of charitable causes. The money kept within the wallet can be invested by WeChat too, so the possibilities to monetize this technology are endless, but also brought some issues concerning security.

**Mini-programs: WeChat’s ‘app killer’**
Mini programs are WeChat’s effort to resolve a seemingly unsolvable problem on mobile devices: people download a lot of apps and spend a lot of time in it, but they only use a very limited part of apps in total. The real advantage of WeChat’s mini-programs is that users do not have to actually download an app and then use them. The mini apps that reside within WeChat can be accessed at any time.
Screenshot 7 – WeChat Mini-apps

Screenshot 8 – WeChat Store
This eliminates user concerns about new apps taking up device storage and is also a benefit for brands too. Consumers are looking for to use a much wider variety of mini-apps within WeChat in future. It is somewhat similar to Google’s Accelerated Mobile Pages initiative, or Android Instant Apps. But unlike them, the mini-apps is not open source but are restricted to WeChat, which makes the functionality safer and stronger to security attacks. Users are so engaged as WeChat has been setting partnerships combined with some of China’s biggest retailers (such as JD.com, an Amazon equivalent) via mini-apps.

WeChat has built its success on integrating everything into its users’ daily lives and combining all of the most popular brands and services, which is all tied together through a reliable, seamless payments system. Business men tend to place advertising first, but WeChat has so far achieved huge success by doing the thing another way around, without exploitation of the potential of platform’s advertising. By first developing an engaged user base, it is now in the highest position to provide them with useful advertising.

As I mentioned above, those special features and functionalities make WeChat powerful but also complicated and vulnerable. It could be a double-edge sword to customer when security problem occurred. So that the research is to figure out what forces and factors could affect user’s information security awareness under such complicated operating environment.

All semi-structure interviews are conducted around users in this mainstream SNS since users spend a lot of time using the apps every day, so that they are well experienced and capable enough to answer my questions with their using experience. Which is very important for the researcher to understand human thought and action in interacting with social network services. And then stimulate the potential to produce profound insights of the lack of security awareness among SNS users in China. The research strategy is unfolded in next part to make clear which is the methodology to acquire the needed knowledge for answering the research questions.

3.7 Evaluation Criteria of the Research
The evaluation criteria suggested by Lincoln and Guba (1985) is adopted in order to make sure the quality of qualitative research, including trustworthiness, credibility, dependability, transferability, and confirmability.

Credibility refers to the accuracy of recording the phenomenon that is under investigation. Shenton (2004) emphasized that it is very important to create familiarity with the participants or in other words a friendly environment before start collecting the first data. In this study, the researcher makes a short introduction and discussion before starting data collection in order to create a friendly environment for participants. The
discussion associates with user's general impression of WeChat, broad sense of security issues and awareness, and so on, which aims to create a high level of trust amongst us.

Dependability refers to the steadiness of findings over time. Dependability answers the question whether research results would be the same, were the study replicated with the same or similar participants in a similar context. Under the quantitative research context, changes of methods and techniques might endanger reliability. Corbin and Strauss (1990) point out the reason that researchers must take precautions against instability caused by drift, shifts in hypotheses, methods, and constructs. On the contrary, changes in hypotheses, concepts, and even the focus of a research project are a sign of a maturing and successful research process in qualitative research. As qualitative studies often feature an emergent design, these changes are expected, but researchers need to keep track of them. Detailed and comprehensive documentation of the research process and every methodological decision ensure the dependability of research findings. In this case, memo writing is adopted so that changes or problems are recorded as memos, which makes evident how the research advanced and how I produced evidence that allowed construction of the result in the process and keeps track on them.

According to Corbin and Strauss (1990), transferability refers to determining the extent to which findings can be utilized in other contexts or with other respondents, the similarity between sending and receiving context. In the effort of reducing contextual specificity, a majority of quantitative studies randomize participant selection. For most qualitative studies, participants are selected purposefully. In this case, the participants are selected randomly from all over China by posting information in other Chinese social media. All eight participants are from six different provinces and cities. They are all first meet with the researcher and do not know each other before.

Equivalent to objectivity, confirmability concerns with the issue of bias and prejudices of the researcher. Data, interpretations, and findings are supposed to be secured in individuals and contexts apart from the researcher. When conducting quantitative research, objectivity is rooted in methods. Following the process correctly ensures that findings are independent of values, motives, or political beliefs (Corbin and Strauss, 1990). A continuous study and re-examination of the data ensured that all the findings are absolutely in the same line with participants’ experiences and ideas and not with researcher preferences and beliefs.

### 3.8 Ethical Consideration

In this study, it is going to collect data regarding our subject directly from the real world. Ethical issues require careful handling to eliminate unwillingly exposing information concerning the third party, controlled by the researcher and most likely by their research institution.
The main purpose of data collection is to get quality of information that gives enough data analysis for building conclusive and reliable answers. And during research process it is researcher’s obligation to keep the ethics in his/her mind because every research possesses several ethical challenges (Taylor and de Vocht 2011; Mellor et al. 2013). While doing research if someone doesn’t want to participate in the research, the researcher should honour his or her privacy. The object of the study is SNS users in China, so permission should be signed before conducting interview. The interviewer should not manipulate interviewees' opinion, and need to be careful about sensitive and challenging questions because it might cause mood fluctuations.

To be systematically, according to Creswell (2003), three important ethical issues are emphasized below:

**Ethical consideration in data collecting:**

Before data collection, the researcher has established connections with participants that were willing to collaborate. The respondents that agreed to participate in this research have written special nondisclosure agreements.

The data collection procedure has guaranteed that the participants involved in this research process are kept completely confidential. All information regarding their personal identity is completely anonymous.

**Ethical consideration in analyzing and interpreting the data:**

The data analyses represent certain beliefs that the respondents hold, however, no specification of the setting or the participants is given. Interpreting the data fully protects the anonymity of the respondents and the confidentiality of them.

Owning the data is a particular concern for the third party. The researcher does own the data, but none of it is made public. The data is saved anonymously, in which the participants involved can never be traced.

**Ethical consideration in disseminating the research:**

This thesis is published and can be accessed by the public at any time in Diva. In this thesis, the reader will not confront the issue whether the researcher has favored one individual against another. Threats to the validity of the conducted research do not exist.
4 Data Analysis

As a researcher of this study, I followed the systematic steps of Lichtman (2010) as regards the analysis of the qualitative interview data that were previously unfolded. The collected data were extensively analysed and examined multiple times in order to identify themes and concepts.

The Three Cs approach gives me a very detailed guideline to organize and analyze my collected data. First of all, I went through carefully many times the transcripts and recordings of interviews. And then, started creating some coding. In the initial coding, users and participants own words used in this phase. Subsequently, during the coding process, I produced many codes and omitted various unnecessary contents. I did this back and forth until I get the desired coding. After that, having decided and created the list of codes, I needed to organize them into categories (Lichtman, 2010). In process from initial list of codes to categories and central ideas, I refined and differentiated the categories resulting from initial coding. I used some of the codes as main categories and changed the names of some categories, removed redundant categories, decided to keep the most significant categories, and developed relations between them. The categories that are treated as essential are repeatedly verified against the text and the data. At the last step, from categories to concepts, some strongest concepts had to be recognized and decided. The final concepts should be one central category and one central phenomenon (Lichtman, 2010).

In this research, all participants were ask about issues concerning the information security issues of WeChat. The interview guide mentions factors may have impact on user’s security awareness forming in term of PMT, and few illuminating questions (see Appendix B). Each of these is introduced by an open question and ended by a illuminating question. The interview guideline present as Appendix B. In this chapter, the process of data analysis are unfolded and elaborated step by step according to Lichtman’s the three Cs (Coding, Categorizing, and Identifying Concepts).

4.1 The Results of Initial Coding

The first step aims at going from the responses to some central idea of the responses (Lichtman, 2010). For this purpose, I went through voice recording and transform into transcript data over and over again, make sure nothing valuable is left in the very beginning. Units of meaning classify expressions to attach annotations and concepts to them. This procedure serves to elaborate a deeper understanding of the text.

During the process, I developed a large number of codes but some of them was collapsed and renamed, since I had to choose the codes work best for the research. As a
result, around twenty codes result from initial coding. So that, the resulting codes are more abstract than draft used in the very beginning.

The twenty-four codes from initial coding:
1. The user base is very wide, which covers all ages level.
2. A significant channel of tracking friend's activities.
3. Indispensable tool of user's work and daily life, they rely on the app for life, even can be described as a part of their body.
4. Frequently used function except instant messaging: WeChat pay; Moment; Official account platform.
5. User's personal information (browsing history) help for customized advertazing through big data analysis by the company.
6. Third-party links and apps are perceived as the most risky for information security.
7. Third-party links & apps provided by both official brand or unofficial content creator.
8. All third-party content providers try hardly to obtain user's personal profile and information.
9. Participants would pay attention to something concerning personal information or sensitive information.
10. Participants realized that there are many ways to lose control of information and lead to losses.
11. WeChat is so powerful and people could not live without it, so that the app holds to many informations and too concentrate.
12. Participants believe in the utilization of information by Tencent, but not distrusful third-party content.
13. Participants would accept complex verification process for safety.
14. Participants think that individual's control over personal information is limited.
15. Participants believe that the mother company should set up relevant security process to regulate user's behavior.
16. Some participants expect Tencent company to take the most responsibility of protecting user's information.
17. Participants usually believed that ‘WeChat security center’ is useful for users to improve their awareness but they would not spend time on it. Reason: Boring content; Too general content, no targeted.
18. People around them and they would seriously take care of security issues when they encounter the problem.
19. Most of the participants would not take active learning.
20. There are many ways for user to prevent information disclosure or decrease account visibility from cyber criminal, only a few of them would practice the methods.
21. Due to curiosity or compelling content, all of the participants would like to allow third-party apps to require personal information or open the links.
22. Participants believed that the precondition of premium service provided by WeChat is based on personal information gathered from user's like browsing history, user habit and so on.
23. From one of participant who works in internet industry: the organization has a pretty standard process for analyzing user's data, which is normative and guarantee safety to user's information.
24. More users, more data, and more effort the organization would put into information security issues, which may improve service as well.

The result of initial coding is a list of twenty-four codes and categories attached to the text above. After this step, data were broke down for better understanding, and categories were developed by grouping them around phenomena discovered in the data, which are particularly relevant to the research question, and put them into an order in the course of time. Categorizing will treat these codes as basis for further works.

4.2 Categorizing and Identifying Concepts

Categorizing is to refine and differentiate the categories resulting from initial coding. For this step, Lichtman (2010) suggest to continue the iterative process. Remember that the goal in the Three Cs analysis is to move from coding initial data through identification of categories to the recognition of important concepts.

In categorizing process, the categories that are most relevant to the research question are refined from the developed codes and the related code notes. Many different passages in the text are then sought as evidence of these relevant codes in order to elaborate the categories on the basis of the questions mentioned ‘What factors influence information security awareness of WeChat users?’ From the multitude of categories that were originated, the ones refined are those which seem to be most promising for further elaboration.

The final step in the process is from Categories to Concepts. As I read and reread the data, I find that some ideas appear richer and more powerful than others. The collected data were extensively analysed and examined multiple times in order to identify themes and concepts. The extracted identified concepts were six as regards the problematic situation:

1. Essential tool
2. Sophisticated environment
3. User's trust
4. Control power and security responsibility
5. Propensity of learning
6. User’s insecure behavior

Additionally, for exhibiting the process of categorizing and identifying concepts, table 2 shows a detailed relevance between initial codes and concepts in order to provide a better understanding of how concepts are generated to readers.

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Initial codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential Tool</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td>Sophisticated Environment</td>
<td>3, 4, 7</td>
</tr>
<tr>
<td>User’s Trust</td>
<td>5, 6, 7, 8, 22, 23, 24</td>
</tr>
<tr>
<td>Control Power and Security Responsibility</td>
<td>10, 11, 12, 13, 14, 15, 16, 22, 24</td>
</tr>
<tr>
<td>Propensity of Learning</td>
<td>9, 15, 17, 18, 19, 20, 22</td>
</tr>
<tr>
<td>User’s Insecure Behavior</td>
<td>20, 21</td>
</tr>
</tbody>
</table>

Table 2. Summary of Interview Findings

In this section each concepts are presented extensively, a process that is fully extracted by all the participants’ worldviews, perceptions and beliefs.

4.2.1 Essential Tool
It may be hard for people outside of China to grasp just how influential WeChat has become there. According to Thompson (2017), he indicated that ‘For all intents and purposes WeChat is your phone, and to a far greater extent in China than anywhere else, the phone is everything. There is nothing in any other country that is comparable: not Facebook, not LINE, not WhatsApp.’

The most mentioned role of WeChat by participants are ‘daily drive.’ and all of them are taking WeChat as an indispensable tool. All participants emphasize that WeChat has been a very important part of their lives, both work and life. Some of participants even believe that WeChat is more than important, which is like an integral part of their body, as instant communicating with friends or colleagues are both significant during their work time and life time.

All participants said that WeChat pay is pervasive in China both cities and countryside. It is easy to transform a small amount of money to sellers by scanning QR code or transfer money between friends. P1, P3, P4 and P7 stated that WeChat Pay has been an essential way of purchasing method. For example, P5 stated that ‘I use WeChat Pay every morning for buying breakfast on the street, and almost every peddler support this method, which is convenient and fast.’ P3 stated that ‘I transfer money to others through WeChat Pay so often’ P7 stated that ‘I use WeChat to call a taxi all the time, which is like Uber but interpreted very well into a big application and pay directly from the APP,
no need for other payment methods.’ In this case, participants treat WeChat as an essential payment method during work or life time.

Meanwhile, participants spend a lot of time on the app with social sharing function—Moment. All participants mentioned that WeChat is the priority way to track friends' activity and share their stuff, which makes them consume much time on it every day, some of them even think that he/she has social networking addiction. P1 stated that ‘WeChat moment would be the first thing I check everytime when I open the APP. I follow my friend’s situations mainly in this way.’ P6 stated that ‘I check various official account during commute time, which is a good way to kill time and utilize fragmentary time. Official accounts push information and content with different orientation, such as cooking, fitness, stock, business and so on.’ According to 2016 WeChat data report (Tencent, 2016 b), daily active users of WeChat reached 768 million in 2016, made an increase of 35% over last year. Over 50% users spend 90 minutes on it every day. It is important to mention that elderly users are proliferating, which is also noticed by participants. P1, P2, P3, P5 and P8 (5 of 8) emphasize that the elder people of their family start to use WeChat every day, and even spend more time than the younger group.

Additionally, Wang (2017) indicates that WeChat becomes harder and harder for its users to opt out. Overseas Chinese or anyone with relationships in China tend to download the messaging app in order to stay in contact since everyone use WeChat in China. P8 stated that ‘there are nothing in any other country that are comparable: not LINE, not WhatsApp, not Facebook. All of those are about communication or wasting time: WeChat is that, but it is also for reading news, for renting cycle, for paying for meal (try and pay with cash for meal, and you’ll look like a luddite), for accessing government resources, for business.’

Those functions make WeChat more attractive and convenient to other similar apps in the market, which makes WeChat more than just an instant messaging applications, but an essential tool in users’ life. The essential property makes WeChat to be irreplaceable, which means that user’s personal information all stored and concentrated in this app. So that more time users spend on this thing, more information the app store and concentrate, which makes WeChat vulnerable when security problem occurred.

4.2.2 Sophisticated Environment

All participants expressed their perceptions that they are using some other functions more than instant messaging within WeChat. WeChat moment, WeChat pay and official account platform are mentioned most among participants. The implementation of Moments was a particularly significant milestone for WeChat ecosystem, as it brought with it a newsfeed featuring updates from friends and contacts. From then, Tencent has added features and opened up the app to outside developers too. 2017, Tencent added mini-apps to WeChat, creating an app store of sorts: inside WeChat, you can play
games, pay bills, find local hangouts, book doctor appointments, file police reports, hail taxis, hold video conferences, and access bank services. Therefore, defining precisely what WeChat is in 2017 turns out to be a much more difficult task than it seems.

Within the WeChat ecosystem, all of participants mentioned that third party apps, especially unverified links, would be risky with phishing site or some other potential harms. P7 stated that there are two forms of third-party apps provided within WeChat, mini-apps or shared page links. As I mentioned before, the mini-apps is not open source but are restricted to WeChat, which makes the functionality safer and stronger to security attacks. WeChat has also been setting partnerships combined with some of China’s biggest retailers (such as JD.com, an Amazon equivalent) in mini-apps, which makes mini-apps more reliable and safer as it is developed with famous brand.

Meanwhile, P2 stated that there are also some third-party apps shared by links either in moments or chats. These are links that not verified by any authorities and usually, it requires users to provide profile information if they want to access or when they click it. These unofficial links could be so dangerous to user's personal information. All the participants recognized that those could be risky, and they usually do not open this kind of links, but still have some possibility to open links and authorize their profile if they think the content of link is interesting or amusing (the phenomenon is analyzed in ‘User’s insecure behavior’).
P4 and P6 stated that they have a lot of friends within their contact since they use the app both in work life and daily life, which makes their WeChat content so complicated.
For avoiding this problem, P4 stated that ‘I would like to add friends carefully or set group sharing (enable users to share content to a specific group of people) when I post something in moments that I do not want a certain group to see it.’ P6 stated that ‘one device can only log in one WeChat account which is inconvenience for me as I have two account one for work and one for normal use. The only way to solve this is having two mobile devices at the same time. This is why people usually use one account for both work and life time.’

P7 stated that ‘The big difference between Moment and Facebook is that WeChat users can only see the moment and activities posted by their friends. However I can only see the comments and likes made by our common friends. If a user does not accept other’s friend request, then they would not be able to view his/her moments, likes and comments. This function makes Moment a more private sharing place compared with Facebook.’

Additionally, even there are some ways to pretend personal information to be exposed as less as possible, but the fact is that the complexity of users operating environment has also been growing with time goes on. All of participants recognized that there are so many ways to trigger security issues or information disclosure and then leads to small or massive losses for user with the application's ecosystem being more and more complex. P1 and P7 also stated that the WeChat application holds more and more user's information with multiple functionalities, which plants the potential risk that it will be a massive loss once they encounter the security issues. As a result, the concept is named as ‘sophisticated environment’ with recording and text data.

4.2.3 User's Trust
During the interview, it is important to mention that all participants hold the high trust to Tencent company while talking about use and control of WeChat data. The reaction of Chinese users towards this issue is quite different compare to western social media users. For example, P7, who works in one of Chinese top internet company, said that gathering information from users is significant for improving the performance of their product and services. Meanwhile, P7 emphasized that the utilization of user's information has high standard within such high-tech company. All of participants have faith in the company since the security issues they knew usually cause by careless actions of user's but not technological defects of base company.

All of participants express that they do not worry about security problem if Chinese government or Tencent company have access of their personal information. P1 states that ‘I would not worry about this concern like western users if I behaves well on Internet.’ P5 shows some discomfort of it, P5 stated that ‘I might feel uncomfortable if government or the company having control of my data, but I do not think government or the company will do something harmful to me, but protection.’ Through all eight
interviews, none of participants take the rumor of government surveillance an security issue in China.

On the other hand, unverified third-party links and applications are rated as the element has the lowest trust of users. The reason from all of the participants is that such links and apps require users to allow the app to access their information or profile, which makes users feel unsafe. Its unofficial property also increases the possibility of data disclosure or security issues.

According to Shin (2010), trust in social networking service is defined as the willingness of a group to be vulnerable to the actions of another group based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to control or monitor that other group. In SNS, trust is a critical determinant of sharing information and developing new relationships. In this research, trust plays a critical role in determining how users tackle the content provided by big organizations and small third-party creators.

The fact is revealed that security affects behavioral intention through attitude indicates that vendors should establish user trust in SNS security by ensuring that their services
are conducted by users’ expectations. This also implicates that trust plays an important role in constructing user's security awareness. So that this section is named user’s trust.

4.2.4 Control Power and Security Responsibility
This category is identified since P1, P3, P4, P5, P6 and P8 (6 of 8) perceive that individual's power of controlling their information from online criminals is limited and much weaker than the protections by Tencent company and WeChat itself. P6 thinks that individuals are vulnerable while tackling such complex security issues so that the company has to take the responsibility of securing information for users and develop the relevant process to regulate user's behavior. P1 and P5 state that they would accept complex but safer verification process concerning information security issues. All of participants believed that the company should provide better protection because some users think the problem is beyond their control.

In addition, P7 stated that ‘Providing great data protection ability is company’s responsibility to users. So that, the services with better information protection usually attract more users than others, which is a positive cycle.’ P8 stated that ‘having some good habit on personal data protection are important to against attack with low end methods, for example, a stranger try to defraud money by fabricating lies about your family member. But it is nearly impossible for a ordinary user against high-end attack from a hacker. So that, Tencent company has the responsibility to make their service safer.’

Screenshot 12 – Example of Pushing Privacy tip in Facebook
From this aspect, the data reveals that users highly rely on app's protecting, which decrease their attention to the effect of individual's behavior. In this ever-changing internet environment, users should always pay attention to their actions, and people is the one who really uses the technology but not the technology itself.

4.2.5 Propensity of Learning
Dutta & McCrohan (2002) suggested that establishing the concept of network security is important. Users must to actively engaged in education and training that will enhance security awareness. They explained that the organization should be conducting training that will inform the community of specific actions that are necessary to be put in place to protect them against the security threats or violence. Training should involve specific technical equipment that will mitigate information security threat on information system.

From the data collected, P1, P2, P3, P5, P7 (5 of 8) do not know the existence of 'WeChat Security Center,' and others might hear of it but do not really open the page and check what is behind it. P6 state that he/she accidentally entered the ‘Security Center’ once, and he/she thought the content was so boring to read.

They were asked will they willing to learn security tips on the page or through other channels, 6 of 8 participants said that they would not do it, and reasons mentioned mostly are 'boring,' 'time-consuming' and 'indiscriminate information.' Therefore they would not spend time and actively learn security tips. P1 and P8 state that security tips on Internet are obvious and useless, which are basic security knowledge for a ordinary user and does not help a lot.

P1, P3 and P7 (3 of 8) even mentioned that they would pay attention to information security policy only once they encounter security issues while using WeChat. P2 and P8 (2 of 8) stated that they would do preparation before a problem occurred, like searching information security knowledge from Internet and be aware of information protection in their daily using.

4.2.6 User's Insecure Behavior
According to Saridakis et al. (2015), awareness of risky user behavior on social media plays a significant role in reducing cyber criminal. Awareness of risk has been shown to be an antecedent of the intention to perform security behaviors, both in personal and professional contexts. In this case, two kinds of insecure behaviors of user were identified, unaware and aware of actions. Unaware behavior is mainly shown as most of participants do not know the 'WeChat Security Center,' and they would pay attention to security policy only the problem occurred. But aware of insecure behavior of users is also common during the interviews.
Siponen et al. (2007) studied employees’ failure in compliance with the information system security. To address the compliance of the employees, he integrated habit which is the form of the behaviors. The empirical test showed that the habitual information system security with compliance would adaptively persuade the process. He also found out that nearly all the components are positively related to employees’ intention to agree with information system security policies. The result shows that there is a relationship between the two. Significantly, it highlights the reason for addressing employee’s past and automatic behavior so that there will be an improvement in compliance. This study found out why employee is fail to compliance with the information system security under organizational environment. But I found that individual user of WeChat failed in compliance with the security policies they have in mind.

All of participants stated that they would take a risk to open unofficial third-party links or apps if they think it is interesting or attractive for them. The point of it here is that they aware of the risk they are going to take but still willing to take a risk because of curiosity and interest. Meanwhile, P5 and P6 state the ways they can take actions to prevent possible information disclosure or security issues like posting moment content with group showing, not sending sensitive information (at least not whole) or not binding account with cellphone numbers in order to be less detectable from strangers who somehow know user's number. These methods are effective to make the account invisible, but users expressed that they would sacrifice the safety for curiosity or just being lazy.

It is important to mention that some participants would compromise to unverified links for amusing content. P5 state that he/she would click the unsafe link sent by his/her close friend. P8 state that he/she are willing to open the unverified link if the link are spreaded widely by his/her WeChat friends, which makes he/she feel safe about the link.

The category is named as 'User's insecure behavior' and split into aware and unaware two subcategories since the insecure behavior indentified from interview data. Previous research (Saridakis, et al., 2015) also proved that user's risky behavior on social media plays a significant role in reducing online criminals, which also takes a huge impact on the WeChat user's security awareness.

**4.3 Analysis of Interview Findings with PMT**

Six concepts are extract by Lichtman’s (2010) Three Cs methods, there are essential tool, sophisticated environment, user's trust, control power and security responsibility, propensity of learning, user's insecure behavior. To some extent, those finding are still in superficial level. Protection Motivation Theory helps to acquire deeper understanding and finding of the problem, in this case, what factors influence individual user of
WeChat intention when face with a security threat, and also provides the core theoretical foundation for this research. In this section, the influence of six concepts are broken down with PMT.

4.3.1 Essential Tool and Sophisticated Environment
First of all, essential role of WeChat does not have direct impact in terms of factors of PMT, but stimulate the usage time of user, which raise the odds that user expose personal data to potential threats. In turn, a user might be vulnerable and a potential security problem might be severe with usage time increasing. The essential property also makes WeChat irreplaceable, which means that user’s personal information all stored and concentrated in this app. So that more time users spend on the app, more information the app store and concentrate, which makes WeChat vulnerable when security problem occurred. According to Saridakis et al. (2015), their study shows that the overall intensity of social media usage alone may increase the risk of becoming a victim of cybercrime. Therefore, essential role of WeChat influences vulnerability and severity from user perspective.

WeChat’s sophisticated environment also increase vulnerability of user and severity of security issue, but from software perspective. As I have find previously, in this case, individuals use WeChat to communicate and keep in contact with family and friends, but it also has a specific business and professional orientation. Previous research by Junco (2012) proves that popular SNS such as Facebook is often used for reasons other than to socialize.

In this research, WeChat has blurred the lines of personal versus professional use. WeChat’s multiple functionalities are now strongly woven into the fabric of users' daily life. As such, this is now known as the WeChat ecosystem, and it continues to expand into new territories and new aspects of daily life. The more sophisticated environment within WeChat, the more crucial it will be for people's work and daily life.

Additionally, third-party applications pose additional risks. Users may have a false sense of security because of the applications’ association with a site they trust or having interested content. Developers release the vast majority of applications without prior review by the site. As a result, the concept of essential property and sophisticated environment increase vulnerability of user and severity of security issue, which may cause user's failure of having a solid information security awareness.

4.3.2 User’s Trust
In SNS, trust is a critical determinant of sharing information and developing new relationships. Same for the trust under the context of WeChat, trust plays a critical role in determining how users perceive their vulnerability and severity of security issue. According to Shin (2010), trust in social networking service is defined as the willingness of a group to be vulnerable to the actions of another group based on the
expectation that the other will perform a particular action important to the trustor, irrespective of the ability to control or monitor that other group. In human’s daily life, during face-to-face interactions, trust is a significant determinant for sharing information and developing new relationships (Coppola et al., 2004). Trust is also critical for successful online interactions. E-commerce research has found trust greatly related to information disclosure (Metzger, 2004). The higher the customers’ trust in the site, the fewer effort customers will apply to inspect details of the site to assess its authenticity of services. Studies of interpersonal exchange situations confirm that trust is a precondition for self-disclosure since it reduces perceived security severity involved in visualizing private information (Metzger, 2004). Overall, user’s trust toward stakeholders within WeChat significantly influence their perceived severity.

In PMT, perceived severity refers to the severity of the consequences of an occurrence (Maddux and Rogers, 1983). In this context, loss of personal information and online identity are considered as possible consequences. Participants have different trust level toward Tencent company and third-party content by other developers. High-level perceived severity is given to third-party content, in other words, participants have high security awareness when face with unverified links and content, and perceive they will be vulnerable. According to Maddux and Rogers (1983) both perceived vulnerability and perceived severity increase the probability of the maladaptive response. In this case, high-level perceived vulnerability and severity toward third-party content increase user’s secure behavior intention and security awareness.

4.3.3 Control Power and Security Responsibility

In this case, participants’ perception of control power and security responsibility over personal data have significant connection with self-efficacy of PMT. According to Maddux and Rogers (1983), Self-efficacy refers to the person’s confidence in his/her ability to perform the required protective actions. Bandura (1977) indicated that self-efficacy is so important that all processes of psychological change are mediated by changes in an individual’s sense of self-efficacy or mastery. The factor is adapted to verify the respondents perceived ability of protecting personal data.

From previous interview data analysis through Lichtman’s (2010) Three Cs method reveal that participant perceives their controlling power over personal data is much vulnerable than the Tencent Company. Many of participants decide to give away the responsibility to Tencent company and highly rely on protection methods of the app, which decrease their confidence to the effect of individual's secure behavior and negatively influence user's perception of ability to perform the required protective actions. A quantitative study by Milne et al. (2000) has shown that among all PMT independent variables, self-efficacy has the most strong effect on intention.
Saridakis et al. (2015) found out user who have a higher perception of control over the privacy and security of their information on social networking service are less likely to be victimised. Kim (2008) shows that the feeling of security is largely determined by the users’ feelings of control in an SNS system. There are calls from participants on WeChat to introduce tools (e.g., anti-bullying reporting tools) and automatic security measures (such as dual factor identification requests when users log-in from unknown computers) and give greater control to users behavior. So that in this case, user’s perceived control power and security responsibility is significantly connect with self-efficacy of PMT. Low-level self-efficacy of participants reveals when facing with a security issue, coping behavior are not likely to be initiated, in turn, their behavior intention and security awareness will be in low-level.

4.3.4 Propensity of Learning
The correlation between propensity of learning, response efficacy and response cost has identified, which has significant influence to behavior intention and security awareness.

Response efficacy of PMT refers to the efficacy of the recommended behaviour (Maddux and Rogers, 1983). In the context of social media, numerous tips or suggestions are given from cyber-security experts, such as customize privacy options, control comments, avoid accidentally sharing personal details, change password periodically and so on. From interview findings, participants act out that they have low intention to be educated and their level of security training are poor. Regarding the recommended behaviours by Tencent company and other channels, most of participants believe those corny protection actions are ineffective to prevent potential security events, and they will not gain benefits from the it.

It is important to mention that participants’ perception of response efficacy is different with response efficacy of a recommended behavior itself. For example, sharing sensitive data and information is considered variously among participants. To what extent the data and information should be defined as sensitive is also different among participants. So that some effective behavior might be considered ineffective by participants.

Some of participants believe the opportunity costs in adopting the recommended action are high. From interview findings, response cost showed as the inconvenience of changing habits of user and the boring, time-consuming of learning recommended actions. According to Maddux and Rogers (1983), an individual might not be taking action if he/she has to cost a lot of effort for a small amount of benefits he/she perceived.

Response efficacy and response cost are two components of coping process of PMT after self-efficacy. In this case, coping response of participants is considered ineffective
in preventing the threatened aversive outcome, and behavioral intention is in lower level.

4.4 Summary of Empirical Findings

To sum up the data analysis this chapter, as a result, the relationships of six concepts with WeChat user's security awareness have developed, as shown in figure 4.1.

As I have mentioned before, the analysis of findings of the interviews indicated six concepts through three Cs data analysis methods. A list of codes, texts attached to the data collected from interviews was extracted through initial coding, which is shown as twenty-four codes in the form of memos and texts. Data has been breaking down and understood, and codes were developed and put them into an order in the course of time. From Categorizing and Identifying Concepts, twenty-four codes and texts were refined and differentiated in order to identify and classify links between Concepts. Identifying concept was doing at a higher level of abstraction. I elaborate the development and integration of it in comparison to other groups and focuses on potential core concepts and core variables. The six concepts most relevant to the research question are selected from the developed codes and the related memoing notes, including 'Essential tool,' 'Sophisticated environment,' 'User's trust,' Control power and security responsibility,' 'Propensity of learning,' and 'User's insecure behavior.' Additionally, interview findings are also analysed with conduct of PMT. Six identified concepts have correlation with factors of PMT.

Results from the ‘essential tool’ and ‘sophisticated environment’ showed that WeChat’s multiple functionalities are now firmly woven into the fabric of participants' daily life.
The more sophisticated environment within WeChat, the more crucial it will be for people's work and everyday lives. Additionally, third-party links and apps pose additional risks. Users may have a wrong sense of security because of the applications’ association with a site they trust or compelling content. The phenomenon of essential property and sophisticated environment reflect to participants’ perceived vulnerability and perceived severity of PMT. Interview findings of these two concepts reveal that participants’ evaluation of the degree of danger posed by the threat is always underestimated. Rippetoe and Rogers (1987) shown a significant main effect of perceived vulnerability on coping response, in this case, the effect is also proven to be correct, with people who shows low levels also showing decreased intention to adopt a recommended coping response. Which may cause user failure to have a robust behaviour intention and security awareness.

The finding of ‘user’s trust’ established connection with perceived severity and vulnerability. Participants have different trust level toward Tencent company and third-party content by other developers. High-level perceived severity is given to third-party content, in other words, participants have high security awareness when face with unverified links and content, and perceive they will be vulnerable. Both perceived vulnerability and perceived severity increase the probability of the maladaptive response. In this case, high-level perceived vulnerability and severity toward third-party content increase user’s secure behavior intention and security awareness.

The finding of ‘control power and security responsibility’ over personal data provide an in-depth insight with self-efficacy of PMT. As I mentioned, most of participants believe Tencent company should be responsible to their personal data and protect them from potential threats. They are highly rely on protection methods of the app, which decrease their confidence to the effect of individual's secure behavior and negatively influence user's perception of ability to perform the required protective actions. Low-level self-efficacy of participants reveals when facing with a security issue, coping behavior are not likely to be initiated, in turn, their behavior intention and security awareness will be in low-level.

From the finding of the last category 'Insecure behavior', two kinds of behavior identified in general contain aware and unaware of insecure behavior. It is important to mention that participants tend to take conscious insecure actions when the content of links or apps are compelling, which is understood as aware of the unsafe behavior. Although there are practical ways to make the account invisible, users expressed that they would sacrifice the safety for curiosity or just being lazy. Participants would allow risky third-party apps and links to require information would not lead to damaging consequences every time, but the level of user's security awareness will decline with 'no harm result.' Once they encounter the cybercriminal, the losses could be massive.
Therefore insecure behavior also has the adverse impact on user’s behavior intention and security awareness.

The finding of 'Propensity of learning' gave an in-depth insight on user's behaviour intention and awareness. In this research, participants act out that they have low intention to be educated and their level of security training are poor. The finding revealed that participants arbitrarily underestimate the efficacy of an recommended behavior, and they are failed to comply with recommended behavior because of response costs, such as the inconvenience of changing habits of user and it is boring, time-consuming for learning the recommended behaviors. Response efficacy and response cost are two components of coping process of PMT after self-efficacy. In this case, coping response of participants is considered ineffective in preventing the threatened aversive outcome, and behavioral intention is in lower level.

Overall, Protection Motivation Theory helps me to explain and understand that how six indentified concepts influence behaviour intention and security awareness of user. At the same time, PMT has been proved to be valid for this research, which is a powerful theory to understand the individuals’ behaviors based on their perception of threats posed to themselves and their environment.
5 Discussion

This study was designed to collect data and produce knowledge about the security awareness of WeChat users (i.e., randomly selected from all over China), their preferences and their experience of using WeChat while facing security issues as well as the perspectives of how people perceive a specific security problems, in order to find out what factors influence user's security awareness with PMT. Participants were asked to provide information about and their personal views of questions from their different experience and value. Eight persons interviewed for our research and their responses confirmed our objectives of the study. In this chapter, the discussion of the findings in relation to the documents findings takes place.

5.1 Discussion of the Empirical Findings

This research intended to contribute to the extended literature to the potential factors of influencing the security awareness of individual social media users. The whole process of extracting ideas followed seven principle of interpretive research field of Myers (2003) as well as PMT of Maddux and Rogers (1983) adopted as core theoretical foundation of the research. Aiming to understand the extent of WeChat users security awareness and behaviour intention and what factors have significant impact on establishing user’s security awareness were the core value of the study. In contrast of the extended literature review that was provided during the study, it became evident, that a user’s security awareness is constructed or affected by the ability of SNS users identify threats, dangers and risks exist while using it, and how do they respond it accordingly, in order to reduce security incidents effectively. PMT provides an appropriate framework from both threat and coping response, and how do they affect behavior intention.

Based on empirical findings, six factors are identified from interview data, and then analyzed through PMT. Previous research (Rogers & Mewborn, 1976; Maddux and Rogers, 1983) found an interaction between perceived severity and coping response efficacy on intentions to adopt the recommended coping behavior. These studies found that increments in perceived severity of threat resulted in higher behavioral intention scores only when the coping response was considered effective in preventing the threatened aversive outcome. The results of the present study revealed similar trends, but only under conditions of low self-efficacy. WeChat user usually measure themselves are vulnerable to potential threat and it is severe, but coping response are considered ineffective. As a result, behavioral intention and security awareness of user are likely to be low, and failed to follow the recommended behaviors. Thus, the influence of threat response and coping response efficacy depends largely on an individual’s self-efficacy expectancy. In the present research, self-efficacy mainly showed as participants’
perception of control power and protective responsibility over personal data, which reveals that the security awareness is largely determined by user’s perception of control, trust and responsibility toward an SNS system. In line with previous study, this research finds out that it is important in making users more responsible for their personal data. Previous studies that follow a quantitative approach lost many of the social and cultural aspects of research or are treated in a superficial manner. On the contrary, doing qualitative research helps me to understand participants, their motivations and actions, and the broader context within which they work and live. The six factors reveals in-depth insight of threat response and coping response from participant’s perspective, which successfully answer the research question ‘What factors influence information security awareness of Chinese social media users?’ Within six factors, ‘Control power and security responsiblily’ appers to be the most influential one among others since self-efficacy expectancy proved to be the most powerful predictor of behavioral intentions. In addition, the factor also have significate influence on both threat and coping response. Essential property and sophisticated environment of WeChat reveal that in cases of multipurpose dominant social media, the probability of being a cybercrime victim is increasing, which means the more functionality the service has, the more likely users becoming the victim of the cybercriminal.

PMT also explains users' inaction under threat. Participants receive third-party links or scanning QR code all the time. They know that there is always a possibility that an links contains a malware that could lead to damage or loss of important information stored on their devices, since many well-known security attacks have been launched through these two ways. In this case, participants perceive the threat, but sometimes do nothing to avoid it because response cost. Ignoring a frends message would make their friends unhappy, and do not scan QR code may cause inconvenient of their lives. In turn, participants’ security awareness intentionally compromise to insecure behavior or inaction.

During the interview, a phenomenon is noticeable that all participants believed that being aware of potential security issues and having good behavioral intention are vital while using WeChat, but only a few participants have a systematic description about how to secure their personal information and prevent information disclosure from the cybercriminal. This issue is also highlighted with other related studies mentioned on their findings that users normally do not put effort to read the online social services privacy policies and the terms of use (see e.g. Acquisti & Gross, 2006; Luo, 2012; Li, 2013). This phenomenon has been existing both in western SNS and Chinese SNS. Cranor et al. (2006) noticed that users find learning about privacy and reading the privacy policies to be tedious and time-consuming. Some studies also found that quite many users are aware of privacy features and know how to use them, but they do not take actions to protect their information (see e.g. Acquisti & Gross, 2006; Luo, 2012; Li, 2013). For example, Acquisti and Gross (2006) show in their study that the majority of
Facebook users claim to know about ways of managing the visibility and searchability of their profiles, but only a significant minority are unaware of those tools and options. The evidence from findings and PMT analysis proved that WeChat users must actively engage in education and training in order to enhance security awareness by increasing response efficacy. The factor of propensity of learning revealed that training could take users far away from possible security problems and build a strong self-efficacy when they tend to learn initially. There are poor literatures regarding education programme of security awareness towards individual user of SNS, and the present research fill the gap in research field of individual users. In addition, the result elicits implication for WeChat and other SNS providers. The passive attitude towards security learning indicates WeChat is making the inefficient promotion of security policy and knowledge.

Based on Protection Motivation Theory (PMT) framework, this study also achieved to proceed into the adoption of a qualitative research approach based on the Myers’s (2003) seven principles for interpretive field study, that finally resulted a clear view as regards the factors of how WeChat user’s security awareness is affected.

5.2 Discussion about the Applied Methodology

In this case, the research is a basic interpretive qualitative study. The goal of the research is to understand how participants make meaning of a situation or a phenomenon. Therefore, the researcher serves as the filter for the meaning, using inductive strategies with a descriptive outcome. In order to effectively conduct the research process, Klein and Myers’ (1999) seven principles for the evaluation of interpretive research in information systems are adopted.

The seven principles adopted to understand a number of text or text-analogue data and information from both interview and relevant document in order to find out the insight of what factors influence WeChat user’s security awareness and how they are affected associated with PMT. Additionally, the seven principles was followed to conducte and evaluate of interpretive field of research in information system. The principles help me to concentrate on fieldwork and design my investigations more systematically. But it is important to mention that I spent considerable time deriving the theoretical foundations for the research from diverse literature. Even I focused on the seven principles of interpretive field study and qualitative study, since I had to consider each one of the principles systematically and ensures that none has been left out arbitrarily.

The research is concerned with “what factor influences WeChat user’s behavioral intention and security awareness. While the relationships between potential variables and individual’s behavioral intention could be explored on the basis of many theories, I chose protection motivation theory for the purpose. The research focuses on the wider social context to help explain the multiple viewpoints and conflicting social interests that I think as driving the sequence of phenomenon that occurred.
Since I have access to the interview data, field notes and relevant documents of other sources, in this research, principle four (The principle of abstraction and generalization) had an significant influence in giving priority to principles six and seven (The principle of multiple interpretation; the principle of suspicion), which then in turn dove the utilization of principle two (contextualization). The connection between principles six and seven provides the key point for the results.

Subsequently, It needs to be mentioned that, in this research, principle four of abstraction and generalization is the leading role in interpretive research of a hermeneutic nature. This is because hermeneutics makes the philosophical case that no understanding of new “data” is possible without relying on some pre-understanding. Therefore, the combination of seven principles and PMT successfully answer the research question posted in the early of research.

5.3 Practical Implications of the study

In this research, the findings of factors toward security awareness of individual social media user provide significant implications to both user and service providers. Based on the results that the previous chapter indicated, this research works as an example for other researchers which deal with behavioral intention and awareness of individual information system users and more specifically with low self-efficacy and awareness while using social media. Subsequently, the research also provides the strategic framework of seven principles of interpretive field research that ensures that all the thoughts for security issues around WeChat were equally treated and were analyzed systematically by all participants.

Highlighting the academic contribution of this study, it needs to be mentioned that the under examined related studies are conducted more on quantitative study based on theories like TRA/TPB, GDT, PMT and TAM. Their focus are more on information system user in an organization. However, those studies did not take into consideration the individual user and what factors affect their behavioral intention based on participants perceptions. In this study, participants’ perceptions and viewpoints were adopted and finally help to extract six concepts associated with security issue of WeChat. Therefore, it can be said that the results of the study relied more on the system’s users real thoughts, perception and idea, rather on the technical dimensions that how a system should enhance.

From service provider's perspective, the findings of this study provide meaningful implications for SNS providers. The concept of control power and security responsibility implies that SNS providers should build their own forecasting models for users’ intented behaviors. PMT can be embedded to help SNS providers design more effective personal information management tools for WeChat and other similar SNS.
Meanwhile, the limitation is obvious as detailed empirical tests among different populations are not undertaken in this study, which can help SNS providers to formulate different kinds of alerts and rules for specific groups of users. This can be one of the options for future research.

The finding also implies that training could take users far away from possible security problems and build a strong security awareness if they would like to learn. Giving a basic training and making them know the consequence of security threat could make users be fully aware and be conscious of hackers and intruders. It is clear from the research that effective risk awareness education programmes can help improve risk perceptions.

From a cultural and historical perspective, it is also noteworthy to emphasize, that Chinese social media user is considered different with western user when face with service company and government’s data control. In this case, Chinese users do not consider government and Tencent company’s data control a privacy concern, but a effective way their personal data can be protected from cybercriminal and potential harmful attack. From western perspective, Matt Wright (2018), director of emerging markets at AngelHack, a hackathon organization, said that in mainland China, it’s very culturally ingrained that the government has access to citizen’s life essentially, as long as user not doing anything weird and plotting against the government, they’re not going to dig through your data. There are many western reports have same idea as Wright. In this case, privacy concern from big power is turned up side down from Chinese user of WeChat. The implication is that culture and history can make a significant different on interpreting a same phenomenon while doing interpretive field study.
6 Conclusion and Reflection

This chapter summarizes briefly the conclusion of this study, rising in this way the main points of interests and contributions.

The goal of the research is to understand what factors of security awareness affect individual users’ security awareness and behavioral intention while using WeChat. For this purpose, PMT is adopted as theoretical foundation in this research. That deeper understanding derived through the examination of participants perspectives via the conduction of the interviews. Afterwards, the adoption of seven principle of interpretive field research and PMT worked sufficiently as a practical instruction in order to establish six concepts of WeChat users toward security issues that explained how user’s security awareness is affected.

Six identified factors of WeChat user toward security issues are:

- Essential Tool
- Sophisticated Environment
- User’s Trust
- Control Power and Security Responsibility
- Propensity of Learning
- User’s Insecure Behavior

Regarding the research question, the seven principle and PMT adoption contribured fully in the way on how to find out the insight that, on the one side indentify particular factors from participant’s interview data and documents, and on the other side, helps in a systematic way to understand and explain how those factors affect user’s security awareness and behavioral intention.

Among all six factors, it is noteworthy to mention that the ‘control power and security responsibility’ of user over their personal data is the most significant one on influencing the level of security awareness. In this case, this factor is significantly connect with self-efficacy of PMT. Low-level self-efficacy of participants reveals when facing with a security issue, coping behavior are not likely to be initiated, in turn, their behavior intention and security awareness will be in low-level. In line with previous studies (Bandura, 1977; Milne et al, 2000), their finding are also proved valid in the case of individual social media users.

In conclusion, reflecting the ever-changing nature of the Internet environment, this study offers help in understanding individual’s security awareness and in understanding the implications for developing effective ways to prevent user away from cybercriminal. As users embrace SNS as a new way to experience and inform lives, escape from reality, and communicate with others, and as organizations provide enabling platforms
for users, SNS might evolve into a brilliantly effective support for human-being's work and daily life. However, to continue their popularity, SNS have several challenges to overcome, and security issue is probably the most significant one. SNS developers need a better knowledge of individual perceptions regarding the behavioral intention and security awareness.

In addition, the useful remark of this research related with the challenge to have an organized process of research between different perceptions, beliefs, and viewpoints that participants expressed. This was a significant task, due to the fact that the main purpose for me as a researcher, was to consciously be objective and to avoid being biased or prefer mostly on a particular idea that participants expressed than others. Moreover, another one reservation and challengeable task was the arrangement and the scheduling of meeting in order to conduct the interviews. For some valuable idea, I needed to re-interview the participant for more detailed information. However, the communication with all the participants was in the right order and no problems arose on that occasion.

This research urges further exploration of the ways to raise user awareness about the adverse impact of social networking activity, and calls for internal and external interventions (through users themselves or control from Tencent company) to enforce privacy and information security awareness on WeChat or in parallel to other similar SNS, which are currently lacking. I also suggest that social media services should be encouraged to publish security breaches, as it is likely to increase safer use. In this respect, the results of this study help inform the development of SNS user awareness practices, and enhance security mechanisms implemented on social networking platforms. Furthermore, the findings are important to future researchers and scholars who may wish to test similar relationships in different contexts, especially in China.
References


Appendixes

Appendix A Informed Consent (In English)


Researchers: Shen Han (e-mail: sh222yz@lnu.student.se)

Research purpose
The aim of this research is to investigate how WeChat users perceive information security issues and their level of information security awareness. This study will focus on the concept of information security awareness.

Introduction
You are kindly invited to a master thesis research titled "Factors Related to Users’ Awareness of Information Security on Social Network Service in China." The decision to join, or not to join, is dependent on you. In this research, we are investigating WeChat users’ views about their perceptions of personal information security while using WeChat and how do they secure personal information and how are they affected from that. Your participation in this research is completely voluntary, and you may choose to withdraw at any time or refuse to answer any question you do wish. If you, for any reason, have questions about the research in general or about your role in it, please feel free to contact me.

Benefits to participating in the research
As the researcher, I will be greatly assisted from your participation as it is expected to acquire knowledge and insight about user's perception, awareness, and behavior of personal information security while using WeChat. Nevertheless, I cannot guarantee that you will personally be benefitted from participating in this research. However, you may inspire me and also contribute to generating new knowledge or insight of this field work.

Risks and discomfort
The participation in this research does not include any predictable risks or discomforts. The interviews materials will be used for the master thesis’ purposes, and they might be announced or published at relevant sources. I will respect your approval to participate, and I will not share your information to third. Your decision not to participate will also be accepted without ramifications, either now, or in the future.

Data access
The collected information data and the original transcripts will be limited to the researcher, the supervisor and the examiner of this master thesis.
Confidentiality
1) I understand all the above information, and I agree with the statements above.
Yes                                      No

2) I understand that my participation in this research is the volunteer and I have the
right to withdraw any time if I want without having to provide any explanation.
Yes                                      No

I_________________________ consent to participate in the research conducted by Shen
Han. I have understood the nature of this research and my signature below indicates my
consent. By signing this document, I consent to participate in the research, and you can
use the data and information that I will share with you in your master thesis.

Signature (participant)  Date

Signature (Researcher)  Date
Appendix B
Interview guideline
1. How do you describe the role of WeChat in your daily life? And what is your mostly used function except instant messaging?
2. Do you think your personal information on WeChat is safe or not? Why.
3. Do you pay attention to your personal information protection intentionally while using WeChat? To be more specific, are you being careful with third-party links or links from unfamiliar providers?
4. Do you think having a good attention to your personal information is important while using WeChat?
5. From your personal experience, where the security threats come from when use WeChat? Do you have any cases that your information is under threat?
6. How do you secure personal information? Why do you think it is effective?
7. Do you know there is an official page named ‘WeChat Security Center’ for account security issues and provide security tips for users? Are you willing to spend time to read it?
8. Besides this official channel, are you willing to learn relative security policy? Reason?
9. Despite you have understand of such security policy, will you fellow those policies purposefully? If do not, why do not you comply with it even you know it is useful?
10. Up to now, what do you know about security issues regarding WeChat? And do you have more to share with me?