Knowledge Sharing Processes for Identity Theft Prevention within Online Retail Organisations

By

Abdullah

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at the University of Central Lancashire

October 2017

STUDENT DECLARATION FORM

Concurrent registration for two or more academic awards

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution

Material submitted for another award

I declare that no material contained in the thesis has been used in any other submission for an academic award and is solely my own work

Student Name **Abdullah**

Signature of Candidate 

Type of Award **Doctor of Philosophy (PhD)**

School **School of Business**

ABSTRACT

The occurrence of identity theft has increased dramatically in recent times, becoming one of the fastest-growing crimes in the world. Major challenges associated with identity theft related offences include problems of consumers with credit, such as: aggravation by debt collectors; rejection of loans; disturbance in normal lives such as reputation damage; and the psychological disruption of providing personal data to organisations and banks during the investigation. For these reasons, and with the ready access of identity thieves to the retail industry, this problem is acute in the online retail industry, yet there has been insufficient research undertaken in this domain.

This research investigated knowledge sharing processes for identity theft prevention within online retail organisations. An analysis of how individual staff and teams share their knowledge for identity theft prevention in organisations is presented, which includes the investigation of existing barriers in knowledge sharing for identity theft prevention in organisations. A qualitative case study research approach, using the guiding framework proposed by Salleh (2010), was adopted and extended to improve knowledge sharing processes for identity theft prevention in online retail organisations. Three case studies were conducted with leading online retailers in the UK. Data collection included one-to-one semi-structured interviews, internal documents from the researched companies and external documents from various secondary sources. The researcher used the thematic analysis approach using the NVivo software tool and a manual coding process.

The total number of interviews was 34 across 3 case studies, with each interview lasting between 45 and 75 minutes. The participants were selected according to their experience, knowledge and involvement in solving identity theft issues and knowledge sharing. Investigation of internal documents included email conversations, policy documents and internal conversations such as emails and memos from the researched companies.

This study found that knowledge of identity theft prevention is not being shared within online retail organisations. Individual staff members are learning from their experiences, which is time-consuming. Existing knowledge sharing barriers within the organisations were identified, and improvements in knowledge sharing processes in the online retail industry of the UK using the extended framework are proposed.

This research contributes to existing research by providing new insights into knowledge sharing for identity theft prevention. It extends an existing framework proposed by Salleh

(2010) in the new context of knowledge sharing processes for ID theft prevention in the retail industry by simplifying the model and combining elements into a more coherent framework. The present study also contributes by investigating the online retail sector for knowledge sharing for ID theft prevention. The empirical research identifies the barriers to knowledge sharing for ID theft prevention and the weaknesses of knowledge sharing in online retail organisations relevant to ID theft prevention. Finally, this study provides managers with useful guidelines for developing appropriate knowledge sharing processes for ID theft prevention in their organisation, and to educate staff in effective knowledge sharing.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I am thankful to Almighty Allah who bestowed me upon the courage and helped throughout such a long and challenging process of completion of my PhD project. He also made me consistent, passionate and hardworking which is the pre-requisite to complete this long journey.

After that I am grateful to my mother whose constant prayers and encouragement when losing confidence being distracted from my studies, helped me to regain confidence and to come back on track to achieve my goal. I would also like to pay homage to my beloved wife whose constant support and patience boosted my confidence and helped me to focus on my studies. Her sacrifice in bringing up our children alone, while being away from her and the family for such a long time, is commendable.

I also owe thanks to so many other people for the accomplishment of this task. First and foremost, I would like to extend my gratitude to the supervision team: Professor Yusuf Yahaya, Dr Mahmood Hussain Shah, and Dr Mitchell Jonathan Larson, whose constant knowledge and valuable advice and encouragement in the course of completion of my PhD not only broadened my horizons but also helped me accomplish the study project. Moreover, their constructive criticism enhanced my capabilities and challenged me to give my best at all times. I am indebted to all three of them. Many thanks to Professor Waqar Ahmed, whose support and motivation made me focus on the research goal. Also, I would like to thank my parent institution (Shah Abdul Latif University, Khairpur, Pakistan), who sponsored me for my studies in the UK.

If it was not for the generosity of the organisations that granted me access to interview their staff and internal documents, as well as my colleagues and friends who were available for the pilot study, this thesis might never have been completed or written, so thank you for the support and encouragement.

LIST OF ABBREVIATIONS

B2B	Business-to-Business
BRC	British Retail Consortium
CFA	Chartered Financial Analyst
CIFAS	Credit Industry Fraud Avoidance Systems
CRR	Centre for Retail Research
E-learning	Electronic Learning
E-mail	Electronic Mail
FSABRC	Financial Service Authority and British Retail Consortium
ICT	Information and communications technology
ID	Identity
IT	Information Technology
KM	Knowledge Management
KS	Knowledge Sharing
NFA	National Fraud Authority
NFD	National Fraud Database
OECD	Organisation for Economic Co-operation and Development
SET	Social Exchange Theory
UK	United Kingdom
USA	United States America
US	United States

PUBLICATIONS

1. **Abdullah,** Shah, M. H., & Ahmed, W. (2016). Identity theft prevention in online retail organisations: a knowledge sharing framework. *The Business & Management Review,* 8(1), 71-85.
2. **Maitlo, A**., & Shah, M.H., (2015). Knowledge management: stop information security breaches. *Credit Collection and Risk Magazine* (December 2015), 40-41.
3. Akerman, C., Shah M.H., **Maitlo, A.,** & Ahmed, W. (2015) The Role of Pharmacy Replenishment Systems in Decreasing Pharmaceutical Waste in the UK. *Asian Journal of Science and Technology,* 6(6), 1550-1557.
4. **Maitlo, A.,** Shah, M.H., & Abdul, W.S. (2014). Base 64 Algorithm in Conjunction with Substitution Cipher to Enhance Information Security Level. *4th International Conference on Computer and Emerging Technologies,* Khairpur, Pakistan, 137-142.

CHAPTER 1 INTRODUCTION TO THE STUDY

1.1. Introduction

The aim of this study was to investigate and analyse the knowledge sharing processes in an online retail organisation and to extend a knowledge sharing framework for improving knowledge sharing processes in the area of identity (ID) theft prevention. The current chapter starts with the research problem, identifies the research aims and objectives of the study, and raises the research questions, which were investigated along with a description of the justification to conduct the research study. It provides a brief overview of the need for research to investigate knowledge sharing processes for ID theft prevention within organisations. The contributions to a research study in the area of existing research have been indicated, and an overview of each chapter in this thesis has been highlighted, along with the key components of the research process.

1.2. Research Problem

ID theft plagues the retail industry. The biggest challenges related to ID theft associated offences include problems of customers with credit, for example: aggravation by debt collectors; rejections of loans; disturbance in normal lives such as reputation damage; and the psychological disruption of providing personal data to organisations and banks during the investigation (Shah & Okeke, 2011). Enhanced awareness and media reports of ID theft, such as stealing credit or debit card information, bank account details and other valuable personal information of products and organisations, has increased the interest and attention of people, organisations, governments and researchers (Shaobo Ji et al., 2007). Due to these reasons and with the easy access of ID fraudsters to the online retail industry, the current research study analysed and proposed solutions of knowledge sharing for ID theft prevention in online retail organisations.

1.3. Research Aim and Objectives

This research study aimed to investigate and analyse knowledge sharing processes for ID theft prevention within online retail organisations.

The main objectives were as follows:

- To study and analyse ways in which individual staff share their knowledge of ID theft prevention;
- To investigate the knowledge sharing processes for ID theft prevention between teams within and outside departments in organisations;
- Investigation of existing barriers in knowledge sharing for ID theft prevention in organisations;
- To extend a guiding framework for improving knowledge sharing processes for ID theft prevention inside these organisations.

Based on the above research objectives, the following research questions were posed:

1. How do individual staff members share ID theft prevention knowledge with each other?
2. How do different teams share their knowledge for ID theft prevention within and outside their department in organisations?
3. What are the barriers to knowledge sharing for ID theft prevention in organisations?
4. How can knowledge sharing processes for ID theft prevention be improved?

By achieving the above objectives, the current study has contributed to the research by investigating the knowledge sharing processes for ID theft prevention in online retail organisations. Qualitative research methods, using three case studies, were conducted to explore the validity of factors identified in the framework.

Using several sources of information is referred to as 'triangulation' (Yin, 2011). Qualitative methods focus primarily on facts, such as what a person conveys to others, and what they do, which enables the researcher to understand what is going on in a specific process or a situation. Qualitative research methods were efficient at illuminating the issues and turning up possible explanations, particularly an exploration of meaning (Gillham, 2000).

Using the approach of qualitative research, investigators seek to inspect matters relating to the numerous operations of individuals or groups of people. The researcher adopted such an approach for collecting stories for individual operations using the narrative approach. The interviews were conducted with individual staff members as well as staff working in groups or teams to determine how they experience the operations in question (Creswell, 2014).

This research aimed to investigate and analyse the knowledge sharing processes for ID theft prevention within the online retail organisation. The researcher used qualitative research methods as these were more efficient at capturing the opinions, situations and responses of users towards the knowledge sharing for ID theft prevention in the organisations (Bryman, 2013; Myers, 2013). Thus, this study was based on a qualitative research approach including three case studies.

According to Yin (2014), the research design can have five elements. Firstly as, *study questions*, as the case studies are principally appropriate to the 'how' and 'why' questions of the research study. The initial point for the study was an apparently simple question of why online retail organisations are not able to stop ID theft. Such a question creates some other questions (posed above). The research questions set out earlier in the current section also cover the second element that is *the proposition.* In such a case, it is that ID theft is growing due to not sharing knowledge appropriately for ID theft prevention in the organisation. The third element of research is *unit analysis*, which is associated with the statement of what the case is. A case may be a process, a person, an organisation or (as in this study) a project of investigation of the knowledge sharing processes for ID theft prevention in online retail organisations. The boundaries were set for this case to define who (individual staff members, teams, departments or organisations) to include or exclude, and time limits (start and end of the case). The fourth and fifth elements - *relating data to propositions* and *the measures for interpreting the results* – were also well developed in the case studies.

As was noted earlier, the case studies entailed extensive data collection. A comprehensive literature review of the related area of study was conducted (see Chapter 2). Initially, it included ID theft and its types. Methods of stealing personal information and its existing solutions were considered to understand how ID theft is a big problem for individuals and organisations, and how it could be prevented. After that, knowledge sharing and its importance and uses were considered to understand knowledge sharing processes and

their significance in the organisation. The researcher also focused on understanding the uses of knowledge sharing in the field of information security. It also covered the existing barriers to knowledge sharing for ID theft prevention in the organisation. Knowledge sharing for ID theft prevention is included in the literature review chapter to understand the importance and uses of knowledge sharing for ID theft prevention. Several industry reports, white papers, conference papers, journal articles and books were examined to gain a deeper understanding of the existing methods, and their advantages and limitations for knowledge sharing about ID theft prevention.

Additionally, many theories, research frameworks and models were analysed by comparing and contrasting to extend a framework for the current study (see Chapter 3). The researcher found gaps in the existing research by reviewing the literature of the present research in the area of ID theft prevention and knowledge sharing. A review of the literature not only enhances and clarifies knowledge for the topic, but it is essential for formulating the research questions for the study (Yin, 2014). As a result the researcher designed the research questions for the study after conducting a brief review of the literature in the area of the research for investigation and analysing the processes of knowledge sharing for ID theft prevention within the online retail industry. Semi-structured interviews, internal documents from the companies, and various reports published in print and electronic media were used and data was collected from three online retail organisations.

Each case study was based on eight to twelve semi-structured interviews. The minimum number of interviews for this research study project was set at thirty from three case studies. The researcher conducted in-depth semi-structured interviews with individual staff members, employees working in teams or groups in the companies from the top management to more junior staff. In-depth semi-structured interviews were selected for various reasons, for example, those who supported the participant on issues which were significant to discuss and tackle, enabled the investigator to address the question of the research study (Fielding & Thomas, 2001) and were important to save interview time (Duke, 2002). In-depth semi-structured interviews are considered to be easier and more efficient than strongly structured interviews or unstructured interviews while interviewing participants from top management, as they enable the researcher to remain in control (O'Keeffe et al., 2016).

The researcher studied and analysed internal documents to achieve the research aims and objectives. The documents were studied regarding understanding the current processes of knowledge sharing for ID theft prevention in the organisations. Also studied were various conversations, internal reports and emails to find any evidence of ID theft, the reasons for stealing data from individual staff members and organisations, and the real barriers to knowledge sharing for ID theft prevention and steps taken to overcome those issues.

External documents, including news reports of the organisations published electronically or in print, were investigated to find any evidence or clues of ID theft and its prevention processes. These also included the investigation of the websites of the concerned companies for publications about knowledge sharing for ID theft prevention.

The method of analysis used in this study included thematic analysis through a qualitative coding process (Braun & Clarke, 2006). The coding of data for analysis contained the data collected from the participant companies concerned to establish the patterns. The NVivo software tool was used for thematic analysis along with manual coding.

1.4. Significance of the Study

ID theft is a fraud carried out by using the personal information of the victim. It has become a common issue in the banking and business sectors in online transactions and retail purchasing (Fennelly, 2012). ID theft issues are now increasing daily, becoming one of the fastest growing crimes around the globe (Cho & Lee, 2016; Grover et al., 2011). In the United States of America (USA), each year ID fraudsters offend millions of persons. Approximately 20 billion of United States (US) dollars are allocated to fight ID theft crimes in the USA. However, to fight against ID theft, consumers are forced to spend more than 1 billion US dollars, and industries spend 100 million working hours coping with ID fraud (Eisenstein, 2008).

Many government intuitions and private organisations have implemented various standards and policies to combat ID fraud. However, the number of ID theft crimes is still increasing due to the explicit nature of knowledge sharing, which is in the form of policies and standards. Mostly the employees do not follow the policies, or do not even read the policy and other security related documents (Aimeur & Schonfeld, 2011). These issues can be dealt with by the proper use of KM within organisations (Conrad et al., 2012).

Knowledge Management (KM) is in the focus of current research in various disciplines (Musulin et al., 2011). Researchers emphasise knowledge sharing in areas of faster-growing industries such as telemarketing, e-marketing, e-banking, e-commerce, project management and others. For example, I-Ching Hsu et al. (2011) developed a platform for knowledge sharing. Such a platform was based on web feeds for the project management team, with knowledge obtained from different shared resources such as web blogs, web-based multimedia and social network bookmarks.

An important concept in KM is tacit knowledge, which can be enhanced by doing things and experiencing them (Guang-bin et al., 2010). Salleh (2010) developed a model for sharing tacit knowledge in a public sector accounting organisation. The model connected knowledge enablers in the process of sharing in an accounting organisation (Ibid).

The literature describes that, to some extent, research has been conducted on knowledge sharing and ID theft prevention. Several surveys and case studies have been carried out to understand ID theft and how big a problem it is for individuals as well as for the organisations (Stephen Harrison, 2013; Bindra et al., 2012; CIFAS, 2012; CIFAS, 2013; Lai et al., 2012; Sakharova, 2012; Romanosky et al., 2011; Bradford & Cundiff, 2006).

Previous literature describes the various categories of ID theft and frauds committed by ID thieves using different methods (Fire et al., 2014; Bose & Leung, 2013; Lai et al., 2012; Sakharova, 2012; Jin et al., 2011; Bilge et al., 2009). The literature also gives importance to knowledge sharing in organisations. However, in the literature review of this study, the researcher could not find any examples of tacit knowledge sharing applied in the context of ID theft prevention. Sharing knowledge for ID theft prevention is still not fully effective; employees are still not fully focussed on ID theft prevention. As a result, personal information is still being stolen, and organisations are not sufficiently capable of preventing the theft of their valuable information and the information of related persons, and companies are being victimised and are suffering significant financial losses due to fraudsters.

For these reasons, this research is to study, analyse and propose a framework for knowledge sharing processes for ID theft prevention in an organisation. This research aims to bridge the knowledge gap and provide a useful and novel contribution in the relevant area.

1.5. Contribution to the Research

The proposed study is new and original with limited research having previously been done on knowledge sharing processes for ID theft prevention within organisations. In the detailed literature review for the research refinement process in the area of ID theft prevention knowledge sharing, the researcher could not find any examples of research so far where knowledge sharing concepts such as tacit knowledge sharing had been applied in an ID theft prevention context. Knowledge sharing for ID theft prevention is still not fully effective. Individuals and teams are still not fully focussed on ID theft prevention and therefore, personal information is still being stolen. Organisations are not entirely capable of safeguarding their valuable information; they are being victimised and suffer huge financial losses due to ID fraudsters. For these reasons and with the ready access of ID thieves to the retail industry, this research is an attempt to bridge that knowledge gap and provide a useful and new contribution in the area concerned. Section 6.5 in Chapter 6 describes the novel contribution of this study in detail.

This study has investigated knowledge sharing processes for ID theft prevention within the online retail sector which makes it new and unique. The researcher studied and analysed how individual staff members share their knowledge for ID theft prevention with each other, investigated the knowledge sharing processes for ID theft prevention between teams within and outside departments in organisations, and identified the barriers to knowledge sharing for ID theft prevention in organisations.

The present study provided a framework for knowledge sharing for ID theft prevention within online retail organisations, which is a new addition to the research of knowledge sharing in the area of the online retail sector. The framework was extended in the new context of knowledge sharing for ID theft prevention in an organisation. The framework was extended from a conceptual knowledge sharing framework proposed by Salleh (2010). The guiding framework was chosen through appropriate criteria of selecting a guiding framework for extension in the context of the present research study. The criteria for selecting appropriate guiding framework are discussed in detail in section 3.3.

The guiding knowledge sharing framework was used and extended as it connects KM implementers and the process of sharing tacit knowledge in a public sector accounting organisation. It interconnects solutions of KM through culture, leadership, learning and technology to enhance the knowledge sharing process in an organisation. The knowledge sharing model enables the tacit knowledge sharing process and is useful as a process of

strategic KM which supports knowledge networks and knowledge flow to enhance the decision-making process in the organisation. The guiding framework was extended in the new context of knowledge sharing for ID theft prevention in an online retail organisation. The extension of a framework for online retail sector makes this study new and contributes to the online retail sector.

The guiding framework was amended by the removal of additional and complicated factors and adding new relevant factors for effective knowledge sharing processes for ID theft prevention in the online retail organisation. Section 6.5.1 describes the amendments made in the guiding framework in detail. The framework is amended by investigating the researched companies. The changes made in the framework make it effective for enhanced knowledge sharing for ID theft prevention in an online retail organisation, which make this research new, making an effective contribution. Figure 6.3 describes the extended framework of knowledge sharing for ID theft prevention within the organisation.

From the perspective of the practical implications, this research study investigated online retail organisations, identified barriers to knowledge sharing for ID theft prevention, found the weaknesses and provided the solutions for an improved knowledge sharing processes for ID theft prevention. The extended framework can be implemented to enhance the knowledge of individual staff members and teams within and across the departments in the company. Therefore, this study also contributes in the said context.

1.6. Structure of the Thesis

Chapter 2: The literature review chapter covers the study and consideration of the related area of knowledge sharing and ID theft prevention to refine the existing area of research and identify the research gaps.

Chapter 3: This chapter is concerned with the extension of a framework for knowledge sharing for ID theft prevention in an online retail organisation. It includes the compare and contrast method of various frameworks and selects a suitable guiding framework for extension in this research.

Chapter 4: Chapter four is about the research methodology of this study. It contains the research philosophy, relevance and selection of qualitative research and the case studies, along with the case study design and data collection

methods. It also includes the analysis and write-up process. A detailed research plan is given.

Chapter 5: The empirical work of this study is covered in this chapter. The background of the case studies in the online retail organisations in the UK is provided. It includes the selection of the companies, the process of gaining access to the targeted companies, and the processing of the data collection. The findings of the case studies are also provided.

Chapter 6: This chapter includes the analysis and discusses the data collected from three online retail organisations. This study extends the knowledge sharing framework proposed by Salleh (2010) using the theory of KM.

Chapter 7: The conclusion chapter includes the research summary, summaries of the findings of the research questions, key findings, the novel contribution of the present study, the research limitations and the recommendations for future work.

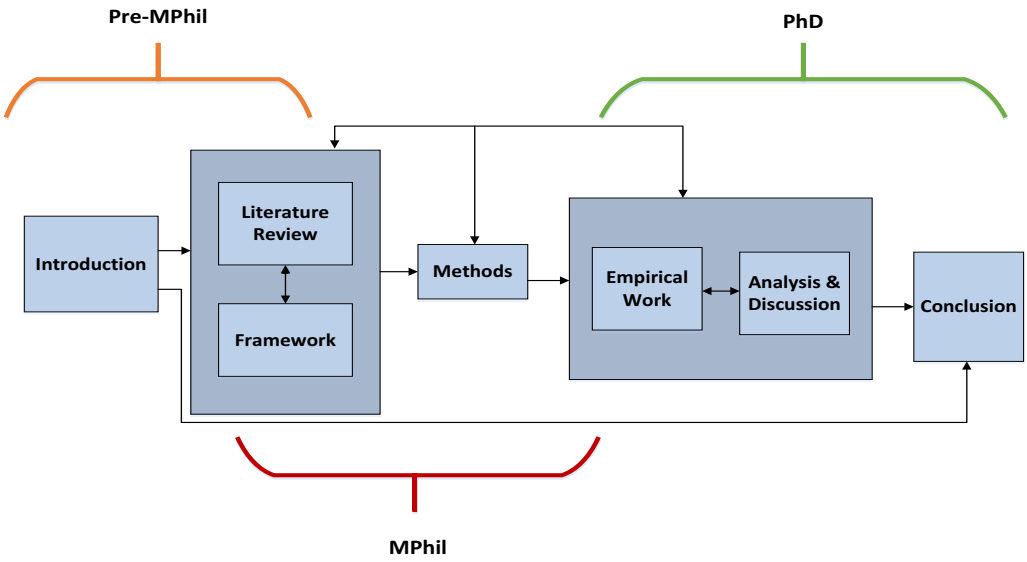

Figure 1.1 Research and development process of the study project

Figure 1.1 describes the structure of the research study project. The research process was divided into three phases of completion. The first step was the pre-MPhil stage of the study. In that phase, the researcher wrote the research proposal and undertook an extensive literature review of the related area of research, investigated existing

frameworks in the field of knowledge sharing and ID theft prevention, and selected an appropriate guiding framework for the present study.

The second phase was transferring from the MPhil to the PhD stage of the study project. During that stage, the researcher designed the appropriate research methods, designed the research instrument, sought ethical approval from the University for the data collection, conducted a pilot study to test the research instrument and prepared for collecting data in the case studies. After the pilot study, the researcher gained access to the data collection for the first case study in *Company X*, collected data, transcribed interviews, and analysed the data gathered from the company, which also included document analysis. The researcher wrote the first case study report and the MPhil to PhD transfer report.

After a successful transfer process, the research moved to the PhD phase of this study project (third phase). The PhD stage included the completion of the remaining two case studies in *Company Y* and *Company Z*, the thesis write-up and the defence for the PhD stage.

CHAPTER 2 LITERATURE REVIEW

2.1. Introduction

The researcher adopted the funnel approached for the research refinement in this study. Figure 2.1 describes the structure of the literature review of this research study, which included the area of ID theft prevention and knowledge sharing, a detailed understanding of ID theft along with its background, and the severity of ID theft issues, describing ID theft methods adopted by fraudsters, and the categories of ID theft. Following that, the stages of ID theft and the existing methods for its prevention are covered.

After the inclusion of literature in ID theft and its prevention, the review moved to knowledge sharing for ID theft prevention and included the importance and applicability of knowledge sharing in organisations, various knowledge sharing approaches, and the challenges of setting up and implementing knowledge sharing systems. Also incorporated was the readiness to setup and apply these approaches to organisations. The review then continues to cover the significance of knowledge sharing to organisational performance and the factors impacting on organisational knowledge sharing.

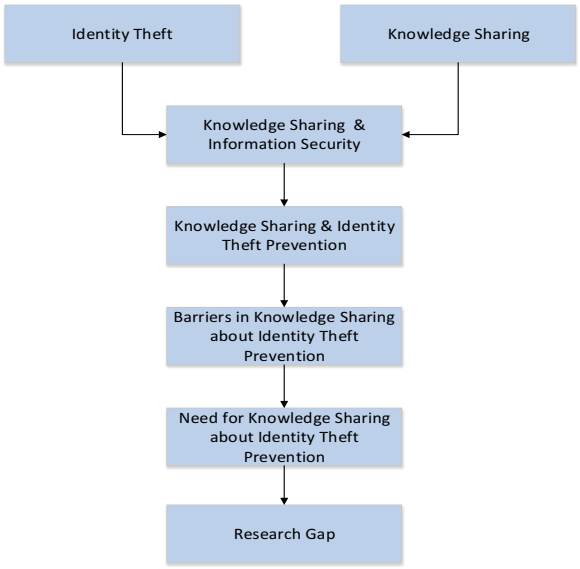

Figure 2.1 Structure of literature review process

It also included significance and the role of knowledge sharing in the field of information security and the existing barriers to knowledge sharing. The review process moved on to

the need for knowledge sharing for ID theft prevention. Theoretical development is also covered in this chapter. After a consideration of the related area for research refinement, a gap in the research is shown.

The literature review was undertaken for the following purposes:

- Establishing the research context;
- Significance of the research question;
- Illustration and description of research done previously;
- To ensure that the investigation had not previously been undertaken;
- To understand the problem structure;
- Demonstrating the researcher's knowledge of the field;
- Synthesising previous perspectives and development of the viewpoint of researcher;
- Gaps and flaws in previous research;
- Point the path forward for future research (about the current study).

2.2. Understanding ID Theft

According to Koops and Leenes (2006), ID theft is a fraud in which impostors steal the information of the victim to commit other crimes. Fraudsters pretend to be other people and steal the information of the victims, and ID fraudsters steal personal information. For example the name, date of birth, social security number, bank account details and insurance details of victims (Hoar, 2001). Fraudsters use that stolen information in unlawful activities; for example, to purchase products and services in the name of the victim and leave them and their bank account with huge bills. As a result, the person whose ID has been compromised may suffer various penalties when the victims are considered accountable for the offender's activities. Due to that reason, in many countries, different laws cover the crime of using the ID of another person for personal interest without the permission of that person (Kolaczek, 2009).

ID theft is considered a serious crime under the law of various countries. However, it is increasing with the advancement of technology and information sharing using internet sources. Mostly, people are not aware that their information can get into the wrong hands and cause them huge losses (Safa & Von Solms, 2016). The information users 'share' on social network websites such as Facebook, LinkedIn and Yahoo, and on any other social

network source, which can be mined and trapped by unauthorised persons (Lam, 2016). As a result, it can cause bank accounts to be hacked or credit card numbers stolen. Thieves can leave their accounts with huge debts by purchasing products in the names of victims (Aïmeur & Schonfeld, 2011).

Table 2.1 ID Theft – Literature review findings

Literature Review Finding	Sources(s)
- ID theft is a fraud in which a victim's information is stolen for another crime.	Koops and Leenes (2006)
- ID stolen includes name, date of birth, social security number, bank account details and insurance details of victims.	Hoar (2001)
- ID theft is increasing with the advancement of information technology. - Mostly people are unaware of the risk of stolen IDs which can cause huge losses for them.	Safa and Von Solms (2016), Reyns (2013), Bindra et al. (2012), and Aïmeur and Schonfeld (2011),
- Personal information shared on social network websites can be stolen and used for illegal actions, which can cause major issues for the victims.	Lam (2016) and Aïmeur and Schonfeld (2011)

Table 2.1 illustrates that ID theft is one of the fastest growing frauds in the world. The literature review identifies that the information of individuals and organisations is not secure enough from ID fraudsters. Information shared on social networks, such as LinkedIn, Facebook, Skype and many other social network websites can be compromised easily and used for several frauds, which can cause significant losses for individuals and organisations.

2.2.1. ID Theft Background

With the advancement of technology, ID theft frauds are also increasing. In the report of the Federal Trade Commission for the year 2006, these frauds were at a high rate of 3.5 per second, and the ID theft crime ratio was 8 million. In 2007 frauds were reported up to 8.1 million. Around 9.9 million consumers lost 48 billions of US dollars in 2009. 11.1 million consumers were affected by bearing the total cost of 54 billion US dollars due to ID theft fraud (Lai et al., 2012).

The survey of the Better Business Bureau released in 2005 showed that an ID thief could be caught once he/she had stolen the ID of 700 people. It also indicated that in 2004, 9.3 million people became the victim of ID theft with a cost of 52.6 billion US dollars and in

16% of cases co-workers, friends and family were involved (Ingram, 2006). According to Romanosky et al. (2011), in the United States of America, customers and businesses lost 56 billion dollars, with 35% of known ID thefts because of breaches in corporate data in one year (2005).

In the National Fraud Database (NFD) of Credit Industry Fraud Avoidance Systems (CIFAS), United Kingdom, 236,516 frauds were documented in 2011. The number of frauds showed a 9% growth as compared to 2010 in the country (CIFAS, 2012). Figure 2.2 shows the number of frauds from 2007 to 2011 as documented by CIFAS.

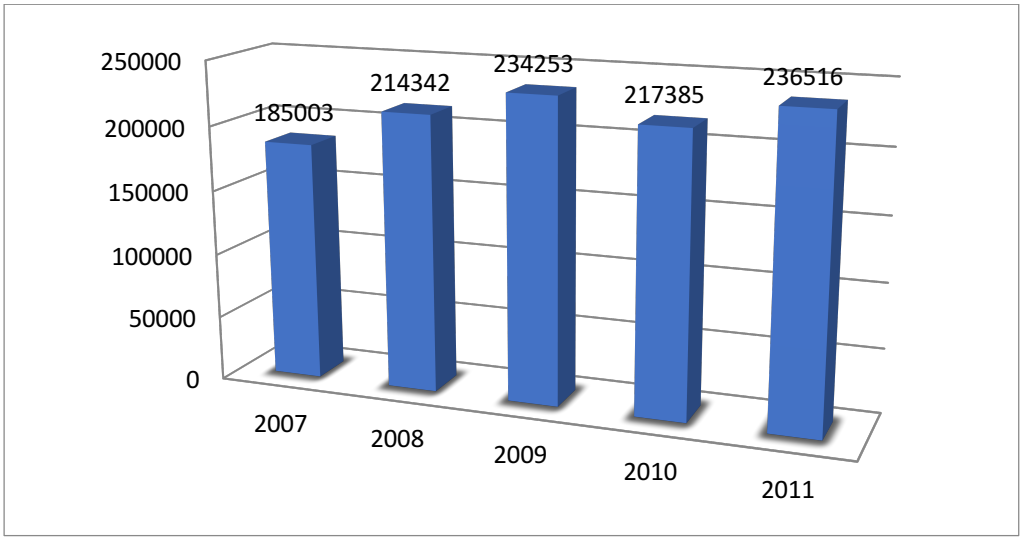

Figure 2.2 Frauds recorded in the National Fraud Database from 2007 to 2011 (CIFAS, 2012)

It is not difficult to fool the system by pertaining to be someone else. It is getting easier and simpler to compromise personal information day-by-day, as it does not essentially need a genius or a computer expert to victimise people by the theft of their IDs. According to Bindra et al., (2012), 10.1 million people were victimised by ID theft in 2011, and every three seconds an ID was stolen.

CIFAS filed 248,325 frauds in the National Fraud Database in the year 2012. The database recorded 123,589 frauds as being ID theft, with a 9.1% growth in the rate of ID theft frauds being committed in 2011. In that year those frauds were registered at 49.8%, i.e. about half of the total frauds committed in the United Kingdom, as shown in Figure 2.3 (CIFAS, 2013).

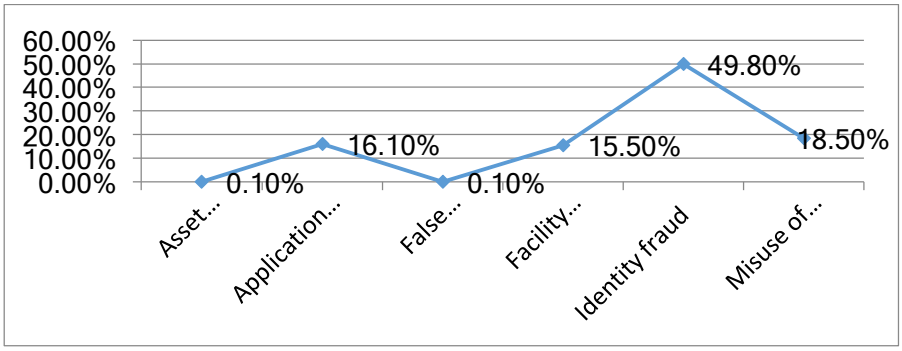

Figure 2.3 Fraud percentage according to fraud types in 2012 (CIFAS, 2013)

CIFAS categorised frauds into six key types, as shown in Table 2.2: ID Fraud, Facility Takeover Fraud, Misuse of Facility Fraud, Application Fraud, Asset Conversion and False Insurance Claims. In 2014, ID theft frauds were at their highest at 276,993. In 2015 these frauds increased by 15.9 % to the largest number of 320,900 in the United Kingdom (CIFAS, 2016).

Table 2.2 Frauds according to types in 2014-2015 and % change (CIFAS, 2016)

Type of Fraud	2014	2015	Change (in %)
ID fraud	113,839	169,592	+49
Facility takeover fraud	18,771	15,497	-17.4
Misuse of facility fraud	105,779	94,001	-11.1
Application fraud	37,960	41,186	+8.5
Asset conversion fraud	323	258	-20.1
False insurance claims	321	366	+14
Total number of frauds	276,993	320,900	+15.9

In 2015, ID fraud increased by 49% as compared to 2014 (see Table 2.2). Figure 2.4 shows that in 2015, 53% of all recorded frauds by CIFAS were ID frauds, which is more than half of all the frauds committed in the United Kingdom in the year (CIFAS, 2016).

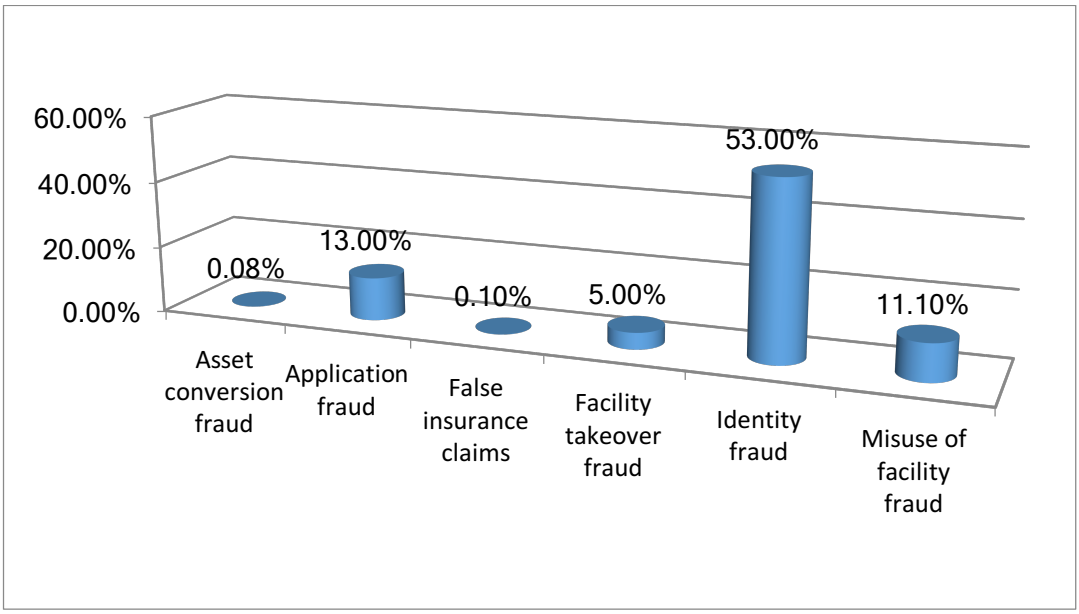

Figure 2.4 Frauds according to percentage in 2015 (CIFAS, 2016)

ID thieves use different methods to steal the personal information of victims, for example:

Stolen or Lost Wallets **-** People carry driving licences, bank and other cards holding personal information in their wallets and often lose them. ID fraudsters use these stolen or found cards in illegal activities. They can then buy products with the names of the cardholder, use the driving licence to commit ID frauds, or sell these expensive cards to other criminals for fraudulent activities (Sakharova, 2012; Bradford & Cundiff, 2006).

Shoulder Surfing - ID thieves observe personal information by looking over the shoulder of a victim when he/she fills in personal information, such as when the victim uses his PIN number on a cash machine or uses a password to open a personal account using an electronic device. This technique is applied in crowded places by fraudsters to obtain the personal information of victims.

Dumpster Diving **–** This is the most common method to obtain the personal information of victims. In this approach, thieves search through garbage to find useful information about the victims, which may include bank statements and other account related information, driving licences, health insurance information, utility bills, and letters and receipts of retail payments through debit or credit cards.

Mail Theft **–** Fraudsters intercept outgoing and incoming mail to companies and individuals, as stolen mail may include bank statements or information of a recently

opened account, for example, medical insurance policies, debit/credit cards, an employee's payroll details, driving licences, and much more.

Imposters - Thieves pretend to be the victim to steal the personal information of others, such as wearing the uniform of the postal service, security employees, or even the police.

Home/Work Place - Family members/friends can steal information in homes. Co-workers and other staff may obtain very sensitive information about persons and organisations, and commit frauds using the stolen information.

Inside Sources - Personal information can be stolen by employees such as their records, payroll, sales statements, salary account statements, and other related information.

Data Breaches - Advances in technology and the emergence of the internet has increased the chances of stealing personal information. Hacking is one high-tech method of compromising the information of individuals and organisations. Hackers can breach the database systems of educational institutions, health care hospitals, banks, insurance companies, and financial institutions etc. to steal personal information.

Phishing – This is a form of electronic ID theft whereby users are tricked through web spoofing techniques and social engineering to obtain confidential information. Impostors are always updating these technologies, for example, using various methods of attracting or hijacking a web browser into surfing fake websites, and a common user may not be familiar with such phishing techniques. Unfortunately, these impostors are growing in number and complexity. Phishing websites are becoming more common day-by-day, and fraudsters are capable of getting e-banking web details automatically, with no action having been taken by the victims (Thabatah et al., 2010).

Table 2.3 ID theft background – literature review findings

	Literature Review Finding	Source(s)
-	Various methods applied to compromise personal information; ID fraudsters are good at victimising individuals.	Bindra et al. (2012), CIFAS (2012), Sakharova (2012) and Bradford and Cundiff (2006),
-	ID theft has been at a peak in the United Kingdom and all over the world over the last few years, and it is increasing.	CIFAS (2016), Stephen Harrison (2013), CIFAS (2013), Lai (2012), and Romanosky et al. (2011),
-	In 2015, ID frauds exceeded 53% of all fraud committed in 2015.	CIFAS (2016)

Table 2.3 illustrates how fraudsters are victimising organisations and individuals. ID frauds have been at a peak in the United Kingdom for a few years, and in 2015 ID frauds were recorded at over 53% of all the frauds committed in the year. People are not fully aware of how to protect their sensitive information from ID thieves. Furthermore, criminals are compromising the information systems of companies. Therefore, research is needed to secure the personal information of individuals as well as the information of organisations.

2.2.2. Categories of ID Theft

ID theft has different categories, which include: Financial ID Theft, Criminal ID Theft, ID Cloning, Commercial ID Theft, Medical ID Theft, New Account Fraud and Account Takeover Fraud.

- **Financial ID Theft**

The fraudulent use of ID when paying for purchases of goods or services using the information of the victim refers to financial ID theft, which can leave huge debts on the accounts of victims. Due to the broader use of plastic cards, thieves have organised themselves with new techniques and methods for this fraud. Financial ID theft has caused the loss of billions of US dollars to industry by decreasing the confidence of customers towards insecure ways of payment (Sakharova, 2012).

The financial effect of ID offences is extensive and has become a hot issue around the world. According to the estimation of the National Fraud Authority (NFA), costs caused by ID theft are up to £1.2 billion per year, and each year these losses are increasing (Stephen Harrison, 2013).

- **Criminal ID Theft**

Criminal ID theft refers to the fraud caused by posturing with the victim's ID, such as performing acts of terrorism, committing crimes and getting special permission to show himself or herself as another person (Lai et al*.,* 2012). The particulars of the victim are delivered to law-enforcement agencies. As a result, the victim is arrested and suffers for a long time until enquiries are completed and clarification is made.

Research into the nature and causes of criminal victimisation have increased significantly in recent times (Pyrooz et al*.*, 2015). The combined low self-control and risky lifestyle

opinion seem to provide a picture into why people are targeted in various ways. No one is secure from ID theft anymore (Gordon et al., 2007). It characteristically consists of compromising the ID of a victim, opening credit card accounts and banking, performing financial transactions for criminal activities, and purchasing illegal products (Holtfreter et al., 2015). This form of victimisation requires examination in the context of increasing the knowledge of individual staff members and employees working in teams for securing personal information to decrease the criminal activities in the country.

- **ID Cloning**

ID cloning refers to using the information of another person and adopting his/her ID in everyday life. It can even be used to establish a new life. The victim's information is used with important cards, special permission and relevant papers related to the victim (Jansen et al., 2016). ID clone attacks have increased due to the emergence of online social networks (Hajli & Lin, 2016). Fraudsters create false identities for malicious purposes and then attack, which affects the trust of the relationships which the victim has developed with other users of the network (Jin et al., 2011).

To commit such a fraud, the attackers focus on going through the profile of the victim and collecting information, for example, name, date of birth, phone numbers, home address, and work related information and pictures. They create a fake ID with the stolen information and then communicate with other users (Fire et al., 2014; Bilge et al., 2009).

ID cloning is the fraud which individuals, as well as organisations, must be aware of; it is something about which family and friends need to be warned, both at home and in the workplace. In contrast to simple ID theft, it is worse than the theft of personal and financial information for specific purposes, for example, to order a product on the internet using the victim's credit card information or Social Security number for getting a job.

ID clones, in fact, pretend to be the victim at all times, 24/7, 365 days of the year. They live and work as the victim. They even pay the bills and live the social life of the victim. They collect more information about the victim so that they can impersonate him/her for years and years. They try to learn where the victim grew up, get knowledge about his/her friends, the centre of religion attended, shopping areas and retail parks usually visited, the dressing style and cosmetics used by the victim. In other words, the fraudsters get all the information that can help them to imitate the victim (Jin et al., 2011).

- **Commercial ID Theft**

Commercial ID theft has become a significant threat to industry and the e-commerce community (Vieraitis et al*.,* 2015) and is amongst numerous cyber crimes that intimidate the security of businesses. Huge numbers of incidents of financially targeted ID theft have surged in current times. This crime is an increasing danger; companies are not sure enough about the payouts acquired from the implementation of ID theft countermeasures (Bose & Leung, 2013). The ID thieves steal credit cards and open accounts with the names of the businesses and apply for heavy loans, higher rents, get vehicles on loan, mortgage houses and other offices and so on (Patil & Dange, 2016; Shaw et al*.*, 2016).

Commercial ID theft occurs when fraudsters use the details of an existing business; for example, they use the name of the business to obtain credit. They can bill the company's clients for the fraudulent purchase of products and services. The fraudster may steal the social security number of an employee of the business or an officer from the management of the company to commit commercial ID theft (Hille et al*.*, 2015).

One point to be worried about is that identifiers such as national identities or employee national insurance numbers are freely accessible in public records, dumpsters or within banks and other creditors; it is not too difficult to access these personal identifiers for commercial ID theft. Commercial ID committers frequently are the employees (current or former), having direct access to the records and financial documentation of the business, and these traitors have ample chance to develop the files for conducting the frauds.

The victims of commercial ID theft do not usually find out about the crime until huge losses accrue or an audit arises and identifies divergences on the record books, due to the hidden nature of these business transactions. Companies can lose huge amounts of money as Commercial ID theft can remain unobserved for some years.

- **Medical ID Theft**

Medical ID theft is used to get care on the health insurance of a victim. Fraudsters obtain the personal information of patients; for example, the medical insurance number and medical claim information of the victim. They then use the stolen information in fake claim benefits by pertaining to be the victim (Kumar & Kumar, 2016; Gregg, 2013).

The trend of medical ID theft is growing gradually. Privacy attacks to victimise famous and ordinary people across the world are more usual these days. Fraudsters find billing

information for patients for financial advantage (Taitsman et al., 2013). In 2012, the Centres traced about 300,000 compromised Medicare recipient numbers for Medicare and Medicaid Services (Agrawal & Budetti, 2012). Around 77,000 complaints about health information privacy breaches were received by the Office for Civil Rights in the United States. They completed 27,000 inquiries with the result that more than 18,000 corrective actions were taken (Health & Human Services, 2012).

Health information security breaches cause a heavy financial loss to the patients. Exploitation of cover identifiers pulls money that could be better used for funding appropriate medical services. Taxpayers bear huge losses when Medicare pay extra for services provided. Medical policyholders face higher payments and co-payments when insurance companies pay extra due to the wrong claims in the names of victims. More clearly, it impacts on the individual beneficiary as a financial liability of victims for the services, which are obtained fraudulently in the name of the recipient. As a result, the beneficiary may suffer from the cut in service limits when the patient looks for reimbursable medical facilities.

- **New Account Fraud**

New account fraud is the form of ID theft in which ID thieves use the personal identifying information of a victim for purchasing products and services using his/her real credit history. This fraud frequently uses the target's Social Security number. Opening new utility, mobile phone and credit card accounts are also common practices of new account fraud (Graves et al., 2016).

- **Account Takeover Fraud**

Account takeover fraud is common in the UK, where fraudsters use the account numbers of victims. For example, a credit card number is used to buy products and services in existing accounts or issue funds from the bank account of the victim. Fraudsters can modify the records of the account of the victim, transfer money to the account of a dead person and then withdraw the balance. Fraudsters even open an account with suitable funds predestined for many administration schemes, with loan approvals to fabricated people, for example, to organise an account takeover (Saha et al., 2016; Patil & Dange, 2016).

2.2.3. Stages of ID Theft

This depends on the description of ID theft; the common type of ID theft is credit card fraud of different kinds. The literature shows that the number of credit card frauds using the internet and the telephone is increasing (Joe Laidler et al., 2016) due to the opportunities provided by the environment of internet usage. However, some exclude credit card fraud from ID theft, as subsequently it can happen only once as it can be exposed rapidly by the credit card company even before the cardholder knows about the fraud. On the other hand, ID theft frauds such as account takeovers are more complicated and take a longer time to solve (Patil & Dange, 2016); these frauds are being committed through the step-by-step process of ID theft.

Newman and McNally (2005) identified three stages of ID theft fraud. A specific ID theft crime may include one or all of the three steps:

Stage 1: The *acquisition* of ID theft by computer hacking, fraud, deception, force, re-directing or capturing mail, or even through legal resources, which includes purchasing the required information on the internet.

Stage 2: *Using* the ID for financial accomplishment, to evade apprehension or hiding someone's ID from law enforcement and other related authorities, such as bill accumulators. At this stage, the frauds include the opening of new accounts, account takeover, or extensive use of debit and credit cards. They sell the ID information on the street and on the black market, and receive additional documents related to ID. For example, a driving licence, passport, visa, health insurance of a victim, tax return applications for huge refunds, stealing leased cars, life insurance fraud, and so on.

Stage 3: *Discovery:* numerous exploitations of credit cards are exposed rapidly. However, "classic" ID theft includes an extensive period before detection, usually from six months to several years. The time taken until discovery is associated with the amount of loss the victim has sustained.

2.2.4. Existing ID Theft Prevention Methods

The quick growth in ID theft cases has increased the attention of researchers, as well as government and non-government private and public organisations. During the literature review of this study, the researcher found that research has been undertaken on ID theft to some extent. Marshall and Tompsett (2005) observed the reasons and approaches for

internet-based ID theft considering how ID theft cases could be identified, examined and legitimated in future and provided recommendations to prevent ID theft by using the problem of trusting relationships and the validation of ID tokens.

Taitsman, Grimm et al. (2013) suggested steps for securing information using mobile devices, which included:

- enabling encryption of data into devices;
- using passwords and other related information for authentication;
- activation wiping and distance disabling to erase information on stolen or lost devices;
- using a firewall to block illicit access;
- installing and enabling well-advanced security software to protect malware-based attacks, spyware, viruses and malicious applications;
- always keeping the security software updated in devices;
- investigating applications before downloading onto mobile devices;
- keeping control of mobile devices;
- enabling enough security to disseminate and receive information while using public Wi-Fi networks systems; and
- removing all information before discarding devices.

Table 2.4 Existing ID theft prevention Methods – literature review findings

Literature Review Finding	Source(s)
Internet-based ID theft is growing at a fast rate.	Marshall and Tompsett (2005)
Securing information through mobile devices could protect ID theft. Steps for information protection in the devices include: - Encryption of data - Passwords and data authentication - Activation of wiping and distant disabling of the devices - Use of a firewall to block illegitimate access - Installation and enabling of well-advanced security software to protect from viruses, malware, spyware and malicious apps - Updating the security software in routine - Investigating apps before downloading onto the devices - Enabling enough security while using public Wi-Fi network systems - Removal of information before discarding devices.	Taitsman Grimm et al. (2013)

The literature indicates that internet based ID theft is growing very fast. Personal information is being stolen from many social network websites, and mobile device users are not familiar with how to protect their information. The literature includes some existing methods to stop ID theft (see Table 2.4), but these methods are not entirely capable of stopping ID theft completely, as hackers steal information, making attacks via viruses, spyware, malicious applications and many more. Therefore, further research is required to design effective methods to fully protect the information of individuals as well as organisations.

2.3. Knowledge Management

Knowledge Management (KM) refers to the process of gathering, storing, processing and disseminating knowledge (Ni et al., 2010). Its purpose is to create and distribute knowledge in organisations or different groups and how to manage the knowledge flow, enabling the organisations to manage their intellectual capital (Pilat & Kaindl, 2011). The KM process can be categorised into knowledge processing and knowledge sharing stages (Nonaka et al., 2000).

Knowledge processing refers to the activities for generating knowledge using different information collection resources, filtering and storing it in various sources, for example, databases and data warehouses (Ur-Rahman & Harding, 2012). The accumulation of employees' knowledge is an important and valuable asset of an organisation. Therefore, the companies tend to keep their employee's knowledge updated. Organisations need enough time during the learning process to train the staff and keep them updated. To deal with such a problem, business organisations usually develop databases comprising explicit knowledge. However, these databases are rarely used due to the massive efforts required to keep them up to date. It is considered to be a process of converting tacit knowledge into explicit knowledge and again converting it back to tacit knowledge in an organisation (Andersen & Broberg, 2016). On the other hand, ***knowledge sharing*** refers to the process of distributing information from place to place using different knowledge sharing sources; an understanding of knowledge sharing is included in detail in the following section.

2.4. Understanding Knowledge Sharing for ID Theft Prevention

Knowledge sharing is considered to be the most important element of KM. The knowledge sharing process enables organisations to increase the knowledge of individual staff members and teams, which leads to the firms having an advantage (Chen et al., 2011). Knowledge dissemination is the flow of knowledge from the *knowledge owner* and *knowledge demander* (Wei'e, 2011). In the process of knowledge sharing, knowledge is shared from one person/place to another person/place as per demand for the sake of communication (Allison et al., 2005). It enhances the knowledge of individual staff members and groups working in the organisation.

Knowledge creation and sharing requires the existence of a person or group of individuals having accurate information, useful skills, capabilities and competencies to create new concepts and ideas for innovative products and processes. Knowledge sharing is the communication process to disseminate the knowledge between one or two sectors of the organisation to develop new technologies or products (Yang & Farn, 2009). Furthermore, it can be defined as an organisational unit; for example, a group of people, a working department or a division which shares their experience with others. Systematically generated and organised information and expertise are exchanged between entities (Wong et al., 2003; Argote & Ingram, 2000).

Knowledge can be shared at different levels, for example:

Basic level – at this stage, it is generated, processed and shared by individuals and it cannot be shared without the involvement of persons.

Intra and transnational organisational level - organisations are known to be an entity, inside of which knowledge is being created and shared at this level of knowledge sharing. Therefore, organisational activities, structures and procedures play the main role in articulating and amplifying knowledge created by individuals within the organisation (Duan et al., 2010).

When organisations engage in *inter-organisational* knowledge sharing, they connect to external networks and retrieve the flow of knowledge from other organisations. Different knowledge categorisation techniques are applied in knowledge sharing among many domestic and multinational corporations, competitors' strategic associations and international projects.

Due to the significance of knowledge sharing, it has remained in the interest of researchers over the last decades. Various research papers were discussed, and different models/frameworks were developed to highlight the knowledge sharing process, main knowledge bodies, dissemination channels, and effective elements; for example, knowledge of the individual, intra-organisational and inter-organisational, and communicational levels (Miesing et al., 2007; Chen et al., 2006; Duan et al., 2006; Ipe, 2003).

As discussed earlier, knowledge is personified in people and can be developed by individuals. Individual staff knowledge sharing is necessary for generating and sharing in the organisation at top levels and cannot be transmitted without the involvement of persons who need to learn it. The nature of knowledge sharing can be divided into the categories of explicit and tacit knowledge sharing.

- **Explicit Knowledge Sharing**

Explicit knowledge can be recorded in numbers, words, sentences, mathematical formulae, graphs and charts which can easily be shared as it can be found in written form in books, articles and websites; it can easily be communicated by visual and oral means (Chen et al., 2011; Kikoski & Kikoski, 2004).

- **Tacit Knowledge Sharing**

Tacit knowledge is gained by experiencing the things, activities and processes of increasing knowledge by experiences and it is considered to be one of the main competitive resources of organisations. It plays a major role in the organisation (Nakano et al., 2013; Ardichvili et al., 2003). In KM, tacit knowledge is considered challenging to convey as compared to explicit knowledge. Tacit knowledge owners tell stories of their experiences to convey them to others (Kalid & Mahmood, 2011). As per the knowledge sharing process in an organisation, tacit knowledge is shared among individuals, teams and departments in organisations, and also among the organisations (Cui Guang-Bin et al., 2010).

Table 2.5 KM, knowledge processing and knowledge sharing – literature review findings

	Literature Review Finding	Source(s)
-	The purpose of KM can be known as managing the intellectual capital within organisations.	Pilat and Kaindl (2011) and Ni et al. (2010)
-	Companies usually develop databases comprising explicit knowledge, but those databases are rarely used due to the massive efforts required to keep them updated.	Leyer and Claus (2013) and Ur-Rahman and Harding (2012)
-	Social knowledge network systems are used to connect employees socially in organisations so that employees can be attached to each other and share knowledge and expertise.	Leyer and Claus (2013)
-	Knowledge can be shared at individual, intra-organisational and inter-organisational levels and also at the communicational level.	Duan et al. (2010), Miesing et al. (2007), Chen et al. (2006), Duan et al. (2006) and Ipe (2003),
-	Explicit knowledge is easier to disseminate. It can be recorded in the form of numbers, words, sentences, mathematical formulae, graphs and charts.	Chen et al. (2011) and Kikoski and Kikoski (2004)
-	Knowledge holders could solely share tacit knowledge, such as telling stories, giving interviews and personal discussions.	Nakano et al. (2013), Kalid and Mahmood (2011), Cui Guang-Bin et al. (2010), and Ardichvili et al. (2003),

Table 2.5 summarises KM and knowledge sharing. The purpose of KM can be understood as managing the intellectual capital within organisations. The literature shows that companies usually develop databases containing explicit knowledge. These databases are rarely used, due to the massive efforts required to keep them updated. Organisations design social networks systems so that their employees can be connected with each other and can share their experiences and expertise to enhance the existing knowledge of workers.

Table 2.5 also shows that knowledge can be shared at the individual, intra-organisational and inter-organisational levels and also at the communication level. Explicit knowledge is easier to share as compared to tacit knowledge due to its recordable form. Employees do not follow stored/recorded information properly. Sometimes they do not even read the company's policy and legal documents, so the information they receive cannot be helpful. Therefore, it is necessary to fully share information with persons inside and outside organisations.

2.4.1. Uses of Knowledge Sharing in the Information Security Field

Information is known to be one of the most valuable assets for business organisations in today's advanced world. Securely managing information has become a significant challenge for companies throughout the globe. Organisations must be capable of handling and managing information securely and safely (Mir et al., 2013) and, as recognised by Davenport and Prusak (1998), knowledge sharing is not simple. The knowledge itself is immaterial. It has been described as a combination of values, circumstantial information, experience and expert discernment which helps individuals to evaluate and integrate new experiences and knowledge (Davenport & Prusak, 1998).

An individual is known as a knowledgeable person who has the efficiency to handle information and new experiences, and who can apply that knowledge and the experiences in various situations. Organisational knowledge is the combination of data, information and human knowledge, which is a valuable asset which can be used for better decision-making, enhancing the efficiency of staff and machinery, enhancing business processes and reducing the risk of uncertainty (Jung-Chi Pai, 2006; Sarmento, 2005; Song, 2002;).

As mentioned earlier, knowledge sharing can either be explicit or tacit. A simple description of explicit knowledge sharing is that it can be expressed in words, codified and conveyed by instruction, documentation, or video and audio formats. However, tacit knowledge is comparatively difficult to formally share as it exists in the minds of the knowledge holders and has not been categorised in a designed format (Jung-Chi Pai, 2006). Knowledge can be formed by obtaining or producing it in the organisation (Davenport & Prusak, 1998).

In the context of information security, knowledge creation can be established by the information security experts, who are appointed by the organisations to accomplish activities which increase information security knowledge. They have devoted units in the organisation as they are responsible for these actions or sharing security knowledge information among staff members and updating information security problems (Nandi et al., 2016). Knowledge is shared when people cooperate with each other by sharing their experiences or helping each other. Devoted information security personnel can participate in the periphery, covering activities to improve security knowledge information sharing in organisations.

The organisation can deliver informal information security advisory and consulting facilities in its other areas, arrange workshops, drills and training for sharing security knowledge. The establishment of a knowledge sharing environment is beneficial as the specific knowledge owned by the information security experts is converted into organisational knowledge and shared with the end-users and others (Belsis et al., 2005). Therefore, the knowledge sharing plays a vital part in the field of information security (Ilvonen et al., 2016) so it has remained in the interests of governments, companies and researchers (Feledi & Fenz, 2012; Zhao Sheng-hui, 2010).

These days, information systems play the main role in collecting, processing, storing and sharing knowledge among organisations and persons. Illicit personnel, such as hackers and other criminals, are keen to gain deeper knowledge about the systems, break the poorly secured systems and share valuable knowledge (Mansourov & Campara, 2011). Due to this, the protection of these systems has become essential, and often the solutions to similar security issues are developed again and again (Feledi & Fenz, 2012). Al Sabbagh et al. (2012) proposed a security training platform for people to improve their awareness of security to learn about security models and increase the use of knowledge sharing in security incident reaction process management.

To some extent, knowledge sharing has been investigated in the information security finance literature. Gordon et al. (2003) studied how sharing knowledge across companies impacts on the overall investment level in the product of information security. Gal-Or and Ghose (2005) investigated how the transfer of the knowledge of information security by two companies affects security investments and price competition in the firms. Liu et al. (2011) studied the relationship of security investment decisions and knowledge sharing in two similar firms. Investigations established a technical knowledge sharing management system, and the impact on the enhancement of information security knowledge sharing between different companies has been accomplished; for example, Feledi and Fenz (2012) explored how machine-readable information security knowledge was shared between information security specialists from various organisations, based on a web portal.

Economic influences of information security investments and using technical knowledge sharing management systems on knowledge sharing have been investigated in the research studies mentioned above. Establishing the security knowledge sharing process

in an organisation to increase or sustain employees' information security knowledge has been studied to some extent.

It has been noted to conceptually comprehend the incorporation of information security and the KM methods based on KM ontology (Guo, 2010). Zakaria (2006) presented a framework for basic security knowledge that can be accomplished through knowledge sharing actions. Belsis et al. (2005) investigated the resources of information security knowledge and the role of an information security KM system. A theoretical model to demonstrate the structure of information security knowledge within organisations was developed by ground research containing five companies and five security specialists and advisors.

Table 2.6 Knowledge sharing in the field of information security – literature review findings

Literature Review Finding	Source(s)
- Information is one of the valuable assets for business organisations. Securely managing the information has become a challenge for online retail companies throughout the globe.	Mir et al. (2013)
- Unauthorised persons such as hackers and other criminals are keen to gain deeper knowledge about the electronic systems of online retail organisations. They break the poorly secured systems and steal valuable information.	Mansourov and Campara (2011)
- Knowledge sharing is vital in the field of information security. It has remained in the interest of governments, companies and researchers	Al-Sabbagh et al. (2012), Feledi and Fenz (2012) and Zhao Sheng-hui (2010)
- Various investigations have been undertaken in the information security knowledge sharing field. - Information is still being stolen, and online retail organisations and individuals are not entirely capable of sharing the knowledge of securing information and its resources.	Liu et al. (2011), Guo (2010), Zakaria (2006), Belsis et al. (2005), Gal-Or and Ghose (2005), and Gordon et al. (2003)

Table 2.6 describes how fraudsters are keen to obtain knowledge of the systems used in organisations. Hackers break the poorly secured security systems and steal valuable information, which shows that information security breaches are increasing day-by-day and staff are not familiar with how to protect their information and the information of the organisations. Therefore, research is required to share information security knowledge at individual staff, department and team levels of organisations.

2.4.2. The Significance of Knowledge Sharing for ID Theft Prevention in the Organisational Performance of Online Retail Organisations

The importance of knowledge sharing in any organisation is progressively being considered (Sloan et al., 2015). As a result, knowledge sharing is gradually being integrated into the agenda of management and in the strategic choices of organisations. It is being considered a significant tool to remaining ahead in the competition among online retail organisations (Ensign, 2016; Smith, 2008; Lee et al., 2006).

Various studies have determined that knowledge sharing has brought many benefits for organisations (Chohan et al., 2014; Haas & Hansen, 2007; Matthew K.O. Lee et al., 2006). It helps online retail organisations to maintain their viable competitive advantage and increases the performance of the organisations. Various opportunities can be created by knowledge sharing which can help to enhance the capability of online retail companies to overcome the requirements of the business and produce solutions to problems for the benefit of the business (Reid, 2003). Positively, knowledge sharing is a significant aspect that impacts on the development and performance of retail organisations (Yang, 2007).

The literature also indicates that knowledge sharing can decrease the loss of intellectual capital caused by persons leaving the business. It condenses expenses by lessening and accomplishing the economics of weighbridge in gaining information from external providers, reducing the idleness of knowledge grounded accomplishments and causes an upturn in production by making knowledge accessible more rapidly and easily in online retail organisations (Chohan et al., 2014). Enhanced worker satisfaction can be achieved by facilitating higher personal development and authorisation (Hussain et al., 2004). Therefore, it can be advantageous for online retail companies to enhance the knowledge of individual staff members and teams working in online retail organisations towards ID theft prevention.

2.4.3. Existing Knowledge Sharing Approaches for ID Theft Prevention in Online Retail Organisations

Knowledge sharing is the practice in which knowledge is shared in an organisation. Hsu (2006) proposes three approaches to increasing employees' knowledge sharing in an organisation:

Technology-Based Approach: In this approach, technology is considered the expediter of knowledge sharing inventiveness in an organisation (Pedro Soto-Acosta & Juan-Gabriel Cegarra-Navarro, 2016; Holtshouse et al., 2013). Knowledge sharing can be implemented and increased by the use of ICT, for example using online databases, data warehousing or knowledge repositories and intranets. The strategic adoption of ICT is one of the most commonly adopted managerial practices in organisations (Starovic & Marr, 2003). ICT can make it easier to encourage persons to share their knowledge. The use of internet technology has increased ID theft problems. Therefore, the technology-based approach of knowledge sharing in online retail organisations can be useful for dealing with ID theft issues (Chohan et al., 2014). It can also enhance the knowledge of individual employees and groups to prevent ID theft in online retail companies. By using ICT facilities, staff can share their knowledge of current ID theft issues and provide protection from those problems.

Incentive-Based Approach: In this approach, financial and non-financial rewards uphold knowledge sharing initiatives. A translucent rewards and appreciation system encourages people to share more of their knowledge (Lam & Jean-Paul Lambermont-Ford, 2010). It can be used as a motivational source to encourage staff members to share their knowledge about ID theft prevention in online retail organisations.

Organisational-Based Approach: This is the approach in which structure, procedures, and management expertise simplify the implication of knowledge sharing initiatives (Iqbal et al., 2015). By looking at the issues of ID theft, it can be argued that online retail organisations should be required to build an enhanced knowledge sharing environment (Chohan et al., 2014), where the management of online retail companies is liable to provide support and encouragement to their staff members and groups to share their knowledge for ID theft prevention.

Table 2.7 Knowledge sharing approaches

Knowledge Sharing Approach	Description
Technology-Based Approach	The technology-based approach is considered to be the expediter of knowledge sharing inventiveness in an organisation. ICT can facilitate and encourage persons to share their knowledge. A technological approach is required for knowledge sharing for ID theft in online retail organisations.
Incentive-Based Approach	An approach in which financial and non-financial rewards endorse knowledge sharing initiatives. Rewards and appreciation systems motivate individuals to share their knowledge for ID theft prevention.
Organisational Based Approach	In this approach, structure, procedures, and management input simplify the implication of knowledge sharing initiatives for ID theft prevention.

Table 2.7 summarises the approaches to knowledge sharing. The technology-based approach is used to implement with computerised systems. These systems include various database systems, data warehousing, communication networks and peripherals used to design these systems. The incentive-based approach contains various rewards to increase the motivation of individual staff members to share their knowledge. The organisational based approach is used to initialise and manage the knowledge sharing process in organisations. Therefore, knowledge sharing approaches are required to enhance the knowledge sharing processes for ID theft prevention within online retail organisations.

2.4.4. Challenges in Setting-up the Knowledge Sharing Approaches for ID Theft Prevention in Online Retail Organisations

The review of the literature specifies that the online retail industry has initiated the realisation of the reputation of knowledge sharing (Charband & Navimipour, 2016; Kozlowski et al., 2016; Lai et al., 2016; White & Fisher, 2008). However, many online retail organisations face challenges with collecting, integrating and developing appropriate information and practices (Jonsson & Kalling, 2007; Bhatt, 2002). Even if knowledge is shared, convincing people to deliver and use stored knowledge resources is a challenge (Suppiah & Singh Sandhu, 2011; Ardichvili et al., 2003). With these enhanced additional challenges, either people are unaware of the complicated knowledge sharing expertise, or they are not cognisant of the advantages of such knowledge sharing inventiveness (Ardichvili et al., 2003).

The knowledge sharing process is full of numerous obstacles (Gupta et al., 2000); it is a challenging task to manage the knowledge sharing process (Ritala et al., 2015; Mueller,

2014; Thoben et al., 2001; Gupta et al., 2000). Despite this, there are many advantages related to knowledge sharing, and there may be many circumstances in which knowledge is not shared efficiently. Where the knowledge distribution is always voluntary, it is a big challenge to create an environment in which people are willing to share what they know and implement what others know (Syed Omar & Rowland, 2004). According to Horibe (1999), organisations need to be aware and satisfy the experienced person as to why knowledge sharing is important (Mittal & Rajib, 2015). This procedure will make online retail organisations convene to their importance and willing to share their knowledge. There are several reasons why developing a smooth and efficient knowledge dissemination approach signifies a substantial challenge.

Many of the obstacles to successful knowledge sharing methods are arguably related to the people, as knowledge sharing has a human element as its basis (Donate & Guadamillas, 2015). People are complicated, with different psychological requirements. Carrillo et al. (2004) investigated large construction organisations of the UK in the context of knowledge sharing process, discovering that the four core challenges encountered in employing knowledge sharing in construction organisations were: a shortage of time, the culture of the organisation, a lack of standardised work processes, and inadequate funding. Dainty et al. (2005) underlined three primary obstacles to the formation of a knowledge sharing culture in an organisation and those companies need to overcome these through an active KM approach. These biggest obstacles were: an uncooperative culture, a poor structure of communications, and time restrictions (Mueller, 2014). Robinson (2011) undertook research on KM in large organisations in the UK, inspecting the observations and barriers to applying knowledge sharing. The following challenges were found to be relevant: the culture of the organisation, unstandardised processes of work, time limitations, employee confrontation, a reduced IT structure, little money, the long term commitment of the organisation, a low understanding of KM, and contradictory significances of the requirements for resources.

Egbu (2004) investigated the issues of KM in production companies in the UK by exploring the inconsistency and lack of possession of knowledge vision in companies. According to him, there was an absolute lack of gratitude for knowledge as a significant asset. Businesses in the industry did not encourage a knowledge sharing culture, and there was a lack of suitable approaches and tools for assessing and appreciating this knowledge. There were insufficiently standardised procedures in place, and there was also an

indication of fixed structures of organisation, time restrictions and massive pressure on the main staff who were the knowledge experts. There was a prevalent aversion to, or anxiety for, the use and request for IT tools for KM that is called *"technophobia"*. A few associates of the business only considered knowledge to be an influence decoration, not as the method of growing earnings linked with knowledge formation, whereby shared knowledge remains with the contributor (*Ibid*). There was a lack of a vibrant determination or shared language and connotation of KM in the online retail industry. Information in online retail organisations is not secure enough from ID thieves. However, staff working in these organisations dealt with the customers and the organisational information, and therefore, they were required to have an enhanced knowledge of ID theft issues and how to protect from these matters (White & Fisher, 2008).

2.4.5. The Organisational Readiness to Implement the Approaches of Knowledge Sharing for ID Theft Prevention

Organisational willingness is now a common and extensively used term, with different definitions. Readiness is assumed in a diverse approach by various people and different organisations; for example, the general definition provided in the current literature uses the word 'readiness' as an essential prerequisite for an individual staff member or an organisation to prosper in organisational revolution (Holt, 2000). Iacovou et al. (1995) define organisational readiness as the convenience of the desirable organisational means for implementation. In the literature of knowledge sharing, Jalaldeen et al. (2009) describe readiness to embrace knowledge sharing as the presence of physical and logical structures in the organisation (known as organisational factors) and the enthusiasm of the organisational members (known as individual factors) to accept knowledge sharing.

According to Jalaldeen et al. (2009), the word 'readiness' combines both attitudinal and physical characteristics, where attitudinal fundamentals comprise the level of knowledge, confidence and responsiveness, awareness of prominence, importance and enthusiasm of the workers to employ the programme. Employees, investment in information technology and structured willingness are used to measure the corporeal readiness of the respondents to apply the agenda. Mohammadi et al. (2010) state that knowledge sharing readiness is the aptitude of an organisation, subdivision or work group to efficiently implement, utilise and gain advantage from knowledge sharing.

Therefore, it is essential for online retail organisations looking to implement knowledge sharing processes to examine their businesses to make sure they are prolific and offer advantageous employment (Jayasingam et al., 2016). Online retail organisations need to focus on the readiness for knowledge sharing processes for ID theft prevention.

2.4.6. Role of Individual Staff in Knowledge Sharing for ID Theft Prevention in Organisations

Most organisations are commonly considered to be knowledge oriented organisations which focus on developing and providing knowledge oriented services to staff (Henttonen et al., 2016; Huang, 2014; Luen & Al-Hawamdeh, 2001). This means that knowledge is considered to be the main resource for the companies (Siong et al., 2011; Singh Sandhu et al., 2011; Willem & Buelens, 2007), and therefore, enabling knowledge sharing and improving the management of knowledge are known to be acute challenges in the private sector (Kim & Lee, 2006; Silvi & Cuganesan, 2006). In a knowledge-based economy, the aptitude of companies to generate, share and adopt knowledge, instead of allocating productivity, limits their long-run performance. A growing number of public and private sector organisations are hence creating efforts to set-up KM systems and practices for the useful, effective sharing and use of the knowledge they keep. An expanding body of research has emphasised the significance of knowledge in organisations.

Currently, there is a growing appreciation for the role of individual staff in knowledge sharing, as well as a bigger level of attention paid to the people's viewpoint of knowledge in organisations (Stenmark, 2000). This perception recognises that individuals in companies are those who hold the knowledge (Grant & Baden-Fuller, 2004). Therefore, the significance of successfully sharing knowledge is currently considered to be dependent on the interaction between individual staff members in the company (Wenger et al., 2002).

There is growing empirical proof emphasising the significance of people and individual related aspects as the top priorities in the processes of knowledge in organisations (Andrews & Delahaye, 2000). Amongst these processes, effective knowledge sharing by individuals plays a major role in a competitive advantage and consistent performance of a company (Wang & Hou, 2015; Nonaka & Peltokorpi, 2006; Kane et al., 2005). Hence, effective knowledge sharing can be a major production driver in online retail

organisations (Silvi & Cuganesan, 2006; Gray & Laidlaw, 2002). Along with numerous studies (Chang & Chuang, 2011; Chow & Chan, 2008; Bock & Kim, 2001), the authors accept that knowledge sharing activities are encouraged and implemented, especially at the individual level. The exchange of knowledge is the support that individuals do to the shared knowledge of the companies (Cabrera & Cabrera, 2002). The ability of an organisation to effectively use its knowledge substantially depends on its individuals, who essentially create, use and share the knowledge.

A comprehensive consideration of the aspects affecting knowledge sharing at individual performance levels seems to be missing (Lu et al., 2006). Where numerous studies include the drivers of individual staff knowledge sharing in institutes (Chang & Chuang, 2011; Tohidinia & Mosakhani, 2010; Chow & Chan, 2008), there is a lack of evidence to some extent to advocate understanding the role of individual staff members in sharing the knowledge for ID theft prevention in online retail organisations. This gap in the existing research is highlighted by Lai et al. (2016), Yildirim (2016) and He and Wei (2009), whose research studies claimed that earlier research studies tended to neglect the connections between the approach leading to the focus on employees knowledge sharing and the environment of enhancing the knowledge of individual staff working in online retail companies.

Moreover, most of the research on sharing knowledge focuses on public sector organisations (Titi Amayah, 2013; Singh Sandhu et al., 2011; Willem & Buelens, 2007; Yao et al., 2007). Quite a few empirical studies have been done on knowledge sharing in private companies (Lai et al., 2016; Yildirim, 2016). A particular need is an investigation of how individuals share their knowledge for ID theft prevention in online retail organisations in the UK (Yildirim, 2016; Chohan et al., 2014). As discussed earlier in the current chapter, individuals working in online retail organisations deal with the product, the customers and the organisational information. On the other hand, the literature states that ID theft is one of the major issues in the UK at the moment. ID fraudsters are too fast and too smart at adopting new methods of stealing personal information (Bush, 2016; Madiwalar, 2016).

Table 2.8 Role of individual staff members in knowledge sharing processes for ID theft prevention

Literature Findings	Source(s)
- Knowledge is a key resource for companies. - Individual knowledge sharing is critical for organisations. - The ability of an organisation to use knowledge effectively and extensively depends on its staff members who essentially create, use and share the knowledge.	Henttonen et al. (2016), Wang and Hou (2015), Huang (2014), Siong et al. (2011), Singh Sandhu et al. (2011), Willem and Buelens (2007), Nonaka and Peltokorpi (2006), Kane et al. (2005),and Luen and Al-Hawamdeh (2001),
- Managing the knowledge and sharing it is known to be a big challenge in the private sector.	Kim and Lee (2006) and Silvi and Cuganesan (2006)
- In organisations, the role of individuals in knowledge sharing needs consideration. - A higher level of attention to the people's viewpoint of knowledge in organisations is required.	Grant and Baden-Fuller (2004) and Stenmark (2000)
- Successful knowledge sharing is dependent on the connections between individuals in the company. - There is rising empirical proof of focusing on the importance of individual staff members and their related aspects in knowledge sharing processes in organisations.	Andrews and Delahaye (2000) and Wenger et al. (2002)
- Various studies accept that knowledge sharing activities are encouraged and implemented, particularly at an individual level. - It is the support that individuals give to the shared knowledge of the companies.	Chang and Chuang (2011), Chow and Chan (2008), Cabrera and Cabrera (2002) and Bock and Kim (2001)
- Research studies include the drivers of individual knowledge sharing in organisations.	Chang and Chuang (2011), Tohidinia and Mosakhani (2010) and Chow and Chan (2008)
- Comprehensive attention to the aspects affecting knowledge sharing at individual staff level performance still seems to be missing in organisations.	Lu et al. (2006)
- The gap in the existing research is highlighted. - Research studies claimed that earlier studies tended to neglect the connections between the approach leading to the focus on individual staff members' knowledge sharing and the environment of enhancing the knowledge of individuals working in online retail companies.	Lai et al. (2016), Yildirim (2016) and He and Wei (2009)
- Most research on sharing knowledge focuses on public sector organisations.	Titi Amayah (2013), Singh Sandhu et al. (2011), Willem and Buelens (2007) and Yao et al. (2007),
- Quite a few empirical studies are done on knowledge sharing in private companies. ID fraudsters are too fast and smart at adopting new methods of stealing personal information. - An investigation of how individuals share their knowledge for ID theft prevention in online retail organisations in the UK needs to be investigated.	Bush (2016), Lai et al. (2016), Madiwalar (2016) Yildirim (2016) and Chohan et al. (2014)
- Effective knowledge sharing can be a major production driver in online retail organisations.	Silvi and Cuganesan (2006) and Gray and Laidlaw (2002)
- Individuals are required to enhance their knowledge of ID theft issues and how to secure information from fraudsters.	Yildirim (2016)

Therefore, individuals are required to enhance their knowledge of ID theft issues and how to secure their information from these fraudsters (Yildirim, 2016). As a result, an

investigation into the existing knowledge sharing processes for ID theft prevention is required. It is mandatory to investigate how individual employees share their knowledge of ID theft issues and protect from these matters. To fill these gaps in the existing research, this research intends to study and analyse ways in which individual staff members share their knowledge for ID theft prevention with each other in online retail organisations as the first objective of this research study.

Table 2.8 shows that individual staff knowledge sharing is one of the significant elements of organisations where individuals play a major role in enhancing awareness in the companies. Previously, various empirical studies have been done on individual knowledge sharing in public sector organisations, but only a limited number of studies include the knowledge sharing processes from the perspective of individuals who work in the companies (see Table 2.8). The online retail industry should be investigated in the context of individual knowledge sharing processes for ID theft prevention. The current study intends to fill such a research gap. To this end, the researcher set the first objective to study and analyse how individual staff share their knowledge for ID theft prevention with each other in online retail organisations.

2.4.7. Role of Teams in Knowledge Sharing for ID Theft Prevention in Different Departments in an Organisation

Organisations depend on various kinds of teams and work groups for developing products, expanding services, and accomplishing the required tasks. For the effectiveness of these teams, it is essential to outline the structures and processes of knowledge sharing within the teams within or outside the departments in the organisation (Van Knippenberg et al., 2004; Cohen & Bailey, 1997). Knowledge sharing in teams is vital for enhanced knowledge sharing processes for ID theft prevention in online retail organisations. Several studies have confirmed the advantages of teams that participate in the exchange of information and communications related to tasks in the teams (Tangaraja et al., 2016; Goh, 2002; Allen, 1977).

Effective teams get the benefit of the perceptions, abilities and ideas of other workmates. A well-established team builds a mutual understanding of the organisational perspective by knowledge sharing, superficially for working tasks (Cooney, 2004; Goh, 2002; Hackman, 1987). The former investigation revealed that knowledge sharing outside the

team (within or outside the department in the organisation) has a meaningful connection with performance in the organisation (Vlăduțescu, 2014; Hülsheger et al., 2009; Brown & Utterback, 1985). It is further shown that knowledge sharing, within and outside teams, plays a major role in the success of the businesses (Argote, 2012).

The knowledge for improved performance in teams can be tacit (Chuang et al., 2016), explicit (Zander & Kogut, 1995), or it can personify in practice (Nelson & Winter, 2009). Knowledge sharing is well-defined as the delivery or reception of the information on tasks and issues, know-how, and the feedback of products and processes (Hansen, 2002). In this research study, it is known as knowledge sharing for ID theft prevention. With the verbal communication for related tasks and the interchange of noticeable issues, knowledge sharing contains implicit synchronisation of proficiency (Faraj & Sproull, 2000), and the information of 'who knows what' in the group/team (Rulke & Galaskiewicz, 2000). Knowledge sharing in teams may involve providing information about the tasks to team members or receiving feedback on the work from management. Knowledge sharing can also include the team's awareness for the identification of ID theft issues and protection from these matters.

The knowledge sources provided for the team can be from within the working department or outside the department in the organisation (Chuang et al., 2016). Furthermore, knowledge can be shared from one department to another department, where staff working in one department can share the information with workers in another department of the company, which results in an enhanced knowledge sharing culture in the organisation (Noor et al., 2016). The literature discussed above clarifies that sharing knowledge in teams within and outside the department in the company enhances the knowledge of staff working in the organisation. However, the literature also clarifies that ID theft is one of the major issues for organisations in the UK. Individual employees and groups working within or outside the organisations are not sufficiently secure from ID theft problems (Abdullah et al., 2016).

Table 2.9 Teams sharing their knowledge for ID theft prevention between departments

	Literature Findings	Source(s)
-	It is important to improve the structures and process of knowledge sharing between team groups within or outside the department in the organisation.	Argote (2012); Van Knippenberg et al. (2004) and Cohen and Bailey (1997)
-	Effective teams get the benefit of the perceptions, abilities, and ideas of different workmates working in teams.	Cooney (2004), Hackman (1987) and Goh (2002)
-	A well-established team builds a mutual understanding of the organisational perspective by superficially sharing knowledge about working tasks.	
-	Several studies confirm the benefits for teams and groups participating in the exchange of information related to tasks in the team.	Tangaraja et al. (2016), Vlăduțescu (2014), Hülsheger et al. (2009), Goh (2002), Brown and Utterback (1985) and Allen (1977)
-	Former research revealed that sharing knowledge outside the team/group (within or outside the department in the organisation) has a positive relationship with performance in the organisation.	
-	The knowledge required for enhanced performance in teams can be tacit, explicit, or personified in practice.	Chuang et al. (2016), Nelson and Winter (2009) and Zander and Kogut (1995)
-	With verbal communication for related tasks and interchange of obvious issues, knowledge sharing contains implicit synchronisation of expertise and the knowledge of 'who knows what' in a team.	Faraj and Sproull (2000) and Rulke and Galaskiewicz (2000)
-	The knowledge sources provided for the team can be from the working department or outside the department in the organisation.	Chuang et al. (2016)
-	The knowledge can be shared from one department to another department.	Noor et al. (2016)
-	Staff working in one department can share the information with workers in another department in the company. It results in an enhanced knowledge sharing culture in the organisation.	
-	Individual employees and teams working within or outside the organisations are not sufficiently secure from ID theft problems.	Abdullah et al. (2016)

Table 2.9 summarises the findings from the literature for the role of teams for sharing knowledge in organisations. The literature shows that various studies criticised the importance of knowledge sharing within and outside teams across departments within an organisation. According to previous research, with verbal communication about related tasks and interchange of noticeable issues, knowledge sharing contains implicit synchronisation of expertise and the knowledge of 'who knows what' in the team. Staff working in one department can share information with workers in another department in the company, which results in an enhanced knowledge sharing culture in the organisation.

However, individual staff and teams working within or outside the organisation are not sufficiently secure from ID theft problems.

Therefore, to bridge this research gap, the current research study investigated the knowledge sharing processes for ID theft prevention between teams within and outside departments in online retail organisations (Research Objective 2 in the present study).

2.4.8. Critical Factors in Knowledge Sharing for ID Theft Prevention in Online Retail Organisations

Regardless of the fact that knowledge sharing is required in all kinds of organisations, it is not easy to employ for various reasons. According to Cross et al. (2001) and Allred (2001), it is hard to manage knowledge, but knowledge sharing can be sustained by focusing on particular contextual and organisational aspects that impact on knowledge flow. KM influencing enablers (factors) are organisational tools to purposefully and continuously raise knowledge (Alvarez et al., 2016; Rezaei & Wan Ismail, 2014). These factors can encourage knowledge formation, secure knowledge, and advance knowledge sharing in online retail organisations. Suitable factors can improve the ability of the organisation to share knowledge (Pan & Scarbrough, 1999).

There are a few factors which can lead to the process of sharing and be of benefit to individuals and organisations. For example, the literature review specifies that a few elements have robust motivational power which may impact on the effective employment of knowledge sharing in an organisation. Based on a critical examination of the factors impacting on knowledge sharing, these are: individual (Alamahamid et al., 2010; Wang & Noe, 2010; Riege, 2005; Lee & Al-Hawamdeh, 2002), organisational (Islam et al., 2012; Martin et al., 2010; Xu et al., 2006; Kim & Lee, 2004; Ives et al., 1997), and technological (Argote et al., 2003; Alavi & Leidner, 2001) - all factors which are commonly pointed out in the literature by many investigators (e.g., Islam et al., 2012; Martin et al., 2010; Salleh, 2010; Xu et al., 2006; Kim & Lee, 2004; Ives et al., 1997).

Table 2.10 describes relationships between knowledge sharing and organisational factors. Salleh (2010) developed a knowledge sharing model that connects KM enablers and the process of sharing tacit knowledge in a public-sector accounting organisation, which interconnects enablers of KM through culture, leadership, learning and technology to enhance the knowledge sharing process in an organisation. Moreover, it enables the tacit

knowledge sharing process and is useful as a process of strategic KM which supports knowledge networks and knowledge flow to enhance the decision-making process in the organisation. Xu et al. (2006) studied the impact of organisational elements on sharing knowledge with participants from the Chinese perspective.

Table 2.10 Important factors in knowledge sharing within organisations

Author(s)	Factors	Impact
Islam et al. (2012)	Management commitment, learning and development, and reinforcement	Positive
Salleh (2010)	ICT Know-how and Skills, Job Training, Job Rotation, Feedback on Performance Evaluation, Learning Opportunities, Information Sourcing Opportunities, Leadership Support, Knowledge Sharing Culture, and ICT Infrastructure and Software	Positive
Martin et al. (2010)	Structure of organisation, culture and human practices	Positive
Xu et al. (2006)	Managerial trustworthy behaviour, culture of organisation and flexible structure of organisation	Positive
Kim and Lee (2004)	Structure and culture of organisation and IT	Positive
Ives et al. (1997)	Structure, processes, strategy and IT	Positive

The study deliberates the implications of the factors for framing the strategies of the organisation for enhancing knowledge sharing. It was found that the trustworthy behaviour of the management and sociability and solidarity were two categories of the culture of the organisation, and the flexibility in the structure of the organisation positively impacted on the behaviour of members of the organisation for knowledge sharing. Islam et al. (2012) inspected the impact culture and structure of an organisation on knowledge sharing in Malaysian MNCs. The study involved factors such as learning and development, support and co-operation, management and assurance, formalisation and centralism. The findings of the research showed that learning and development, management commitment and solemnisation were confidently associated with knowledge sharing. Kim and Lee (2004) analysed how the culture, infrastructure and IT in an organisation impacted on knowledge sharing proficiency in public organisations in Korea. They found a significant relationship in culture, structure, IT and knowledge sharing in the organisation.

From the discussion above, it seems that an organisational factor plays an important role and has a positive impact on enhancing a knowledge sharing process in the organisation (see Table 2.10). Obviously, other factors of an organisation influence the application of

knowledge sharing, and therefore, it is essential for online retail organisations to consider these organisational factors when employing knowledge sharing approaches in their organisations. This study looks at the essential organisational factors, which are ICT Know-how and Skills, Job Training, Job Rotation, Feedback on Performance Evaluation, Learning Opportunities, Information Sourcing Opportunities, Leadership Support, Knowledge Sharing Culture, and ICT Infrastructure and Software for the evaluation knowledge sharing processes for ID theft prevention in online retail organisations in the UK.

2.5. Managing Barriers to Knowledge Sharing for ID Theft Prevention in Online Retail Organisations

The literature describes that the management of an individual person's learning to ensure effective knowledge sharing is challenging to handle (MacNeil, 2003), where the organisation follows a management strategy for developing and holding highly talented and motivated staff members who are well known to be important for current and future organisational achievements. Such an organisation attempts to use the staff members' skills and knowledge to create intangible assets which cannot be replaced by their comparatives (Boxall, 1996). Therefore, an individual staff learning process is required to increase the competent human resources in the organisations (Valentine St Leon, 2002).

However, there can be many barriers in knowledge sharing for ID theft prevention in online retail organisations. These barriers impact on the knowledge sharing processes between individual staff members and teams within or outside the departments of online retail organisations. These barriers need to be identified and managed for an efficient process of knowledge sharing for ID theft prevention.

- **Staff Unwillingness to Share their Knowledge**

According to Hislop (2002), the achievement of KM efforts depends on the willingness of staff members to share their knowledge. The attitude of staff members towards knowledge sharing can be aggravated through their perceptions of the impartiality of their emotional bond with an organisation. These perceptions influence the willingness of individual employees to their total obligation to the organisation (Scott Holste & Fields,

2010). Their positive behaviour and attitude impact on sharing knowledge and benefitting the organisation (Sheehan, 2016; Chang & Chuang, 2011).

The argument of Robertson and O'Malley Hammersley (2000) clarifies that employees who have satisfaction in their jobs and commitment to their companies are willing to share their knowledge and believe that the advantages of the organisation are to their benefit. Therefore, the willingness of staff to share their knowledge for ID theft prevention is mandatory and leads the online retail organisation to a knowledge-oriented environment for ID theft prevention.

Table 2.11 Need of individual employees' willingness in knowledge sharing

	Literature Findings	Source(s)
-	The accomplishment of knowledge sharing efforts highly depends on the willingness of staff.	Hislop (2002)
-	The attitude of staff to share knowledge would be provoked by their perceptions of the impartiality of their emotional bond with the effective organisation. These perceptions affect the willingness of individual staff members to their total obligation to the organisation.	Scott Holste and Fields (2010) and Hislop (2002)
-	Individual's positive behaviour and attitude impact on sharing knowledge and benefitting the organisation.	Sheehan (2016) and Chang and Chuang (2011)
-	Employees who have satisfaction in their job and commitment to their companies are willing to share knowledge, and they believe that the advantages of the organisation are to their benefit.	Robertson and O'Malley Hammersley (2000)

Table 2.11 shows that staff willingness for knowledge sharing is necessary for an organisation. Willingness for knowledge sharing is one of the essential elements in the processes of knowledge sharing for ID theft prevention in an organisation. The behaviour and attitude of individual staff members for knowledge sharing is beneficial for any organisation. Therefore, unwillingness is a barrier to knowledge sharing.

- **Lack of Individual Staff Awareness for Knowledge Sharing**

Individual awareness of the knowledge sharing process is an essential element of knowledge sharing (Ismail & Yusof, 2010). In the last two decades, the concept of awareness has raised the attention of researchers into KM (Daneshgar, 2001). Daneshgar considers individual staff awareness to be a tool for improving co-operation and sharing knowledge as a collective process (*Ibid*).

Awareness is seen as a key component for effective implementation of a knowledge sharing programme for employees (Safa et al., 2016; Cong & Pandya, 2003). Staff members, including higher management, must be aware of the significance of an effective knowledge sharing culture within an organisation (Van den Hooff et al., 2003). Awareness of providing for knowledge sharing is a big challenge in the process in an organisation (Zahedi et al., 2016). Any organisation which is in the phase of unawareness does not realise the impact of knowledge against its competitors (Van den Hooff et al., 2003), and therefore, it is a barrier and needs to be handled correctly.

Table 2.12 Need of individual staff awareness in knowledge sharing

Literature Findings	Source(s)
- Individual staff awareness is vital to the accomplishment of the knowledge sharing process in an organisation.	Ismail and Yusof (2010)
- Individual employee awareness is considered to be a tool for improving co-operation, sharing and knowledge in a collective process.	Daneshgar (2001)
- Awareness is considered a key component for the efficient implementation of a knowledge sharing programme for employees.	Safa et al. (2016) and Cong and Pandya (2003)
- Individual awareness is essential for the accomplishment of the knowledge sharing process in an organisation. - Employee awareness of the knowledge sharing process encourages the individuals to share knowledge efficiently and provides the chance for creative thinking to handle complicated issues and understand the mistakes of others.	Safa et al. (2016)
- The obligation of the significance of the knowledge would affect knowledge sharing between individuals, groups and teams in organisations.	Lee and Al-Hawamdeh (2002)
- Staff, including management, must be aware of the significance of sharing knowledge for effective knowledge sharing culture in an organisation. - Any organisation which is at the phase of unawareness does not realise the impact of knowledge against its competitors.	Van den Hooff et al. (2003)
- Awareness providing for knowledge sharing is a big challenge in the process of knowledge sharing in an organisation.	Zahedi et al. (2016)

Table 2.12 shows that lack of awareness concerning knowledge sharing can be an obstacle to the process of knowledge sharing. Individual staff member awareness is essential to the success of the knowledge sharing process in an organisation (Safa et al., 2016). Lee and Al-Hawamdeh (2002) stated the obligation of the significance of the knowledge would affect the sharing of knowledge between individuals, groups and teams in the organisations. Employee awareness of the knowledge sharing process encourages the individuals to share their knowledge efficiently and provides the chance for creative

thinking to handle complicated issues and understand the mistakes of others (Safa et al., 2016). Table 2.12 shows individuals' awareness is necessary for the process of knowledge sharing as it is vital to understand the knowledge sharing processes for ID theft prevention. The literature clarifies that lack of staff awareness is a barrier to the knowledge sharing and it needs to be managed accordingly.

- **Insufficient Learning Opportunities**

An employee learning environment leads companies to the height of success. Such an environment includes procedures resulting in the accumulation of capabilities and skills of employees through routine work (Mohammad Hossein & Nadalipour, 2016), which in the main focus of many companies who consider themselves to be continuous learning institutions to enhance their employees' potential for effective competitiveness in the market. Learning opportunities increase the progress in output by eliminating previous faults and weaknesses in organisations (Harteis et al., 2008).

An advanced employee learning environment enables staff members to enhance their expertise by improving their knowledge to face the complicated problems they face. Many companies provide numerous training opportunities to their staff to keep them updated with work processes and to improve advanced techniques in performing their activities to aggregate their outcomes (Dymock & McCarthy, 2006). Training is one of those learning opportunities.

Job training is of vital importance in knowledge sharing to increase the knowledge of employees in any organisation, and the worker training can be divided into two different categories. One of these two is *General Training*, which refers to the training that affects general human capital and enhances the production of work in all kinds of the jobs, such as training to increase general computer skills and various language training courses (Hortovanyi & Ferincz, 2015). General skills and knowledge can be transferred to job holders in similar organisations, such as companies competing in a similar sector of industry, and to similar employment in the same occupation and skills. The second training category is *Firm-Specific Training* that enhances the knowledge solely in the workplace of the existing organisation. This training is being provided to improve the knowledge of the machines the employees use, and to understand the substructure of the working place and processes that are employed in the firm where the staff member is working. These training sessions are provided to increase the knowledge of the specific

characteristics of the products and the customers of the company or firm (De Grip & Sauermann, 2013).

The lack of a learning environment in any organisation is a barrier to enhancing the knowledge of individual employees and teams (Luu, 2013; Peter A.C. Smith, 2012), which affects the knowledge sharing processes for ID theft prevention in online retail organisations. Table 2.13 summarises the findings from the literature review of the importance and availability of learning opportunities.

Table 2.13 shows that learning opportunities increase the outcome progress by removing weaknesses and previous mistakes in organisations. These are considered to be the key components for effective implementation of a knowledge sharing programme for employees. Learning opportunities in the knowledge sharing process encourage the individual staff members to share their knowledge efficiently and provide the chance of creative thinking to enable the handling of complicated issues and understanding the mistakes of others.

Table 2.13 Need for learning opportunities in knowledge sharing

	Literature Findings	Source(s)
-	An employee learning environment describes procedures leading to increasing the skills and capabilities in routine work	Mohammad Hossein and Nadalipour (2016)
-	Learning opportunities are considered to be a key component for effective implementation of a knowledge sharing programme for employees.	Cong and Pandya (2003)
-	Learning opportunities increase the progress in working outcomes through removing mistakes previously made and the weaknesses in organisations.	Harteis et al. (2008)
-	Organisations provide various training opportunities to their employees to keep them up-to-date and enhance their knowledge.	Dymock and McCarthy (2006)
-	Training is a learning opportunity to enhance technological skills for computer usage and knowledge sharing.	Hortovanyi and Ferincz (2015)
-	Companies also provide training to enhance the working knowledge of their staff.	De Grip and Sauermann (2013)
-	Lack of a learning environment in any organisation is a barrier to enhancing the knowledge of individuals and teams	Luu (2013) and Peter A.C. Smith (2012)

The literature review shows that learning opportunities are important for knowledge sharing in the organisation, and therefore, the unavailability of these opportunities is a barrier in the process of knowledge sharing for ID theft prevention. Organisations are required to manage this barrier for an effective knowledge sharing process.

- **Distrust of Other Staff Members**

The trust of others is one of the main elements in the process of knowledge sharing (Hashim & Tan, 2015; Usoro et al., 2007) which has remained of interest to researchers. Homans (1958) claimed in his Social Exchange Theory (SET), that individual employee interchange reserves through social interchange correlation. The social interchange is categorised by indeterminate personal responsibilities, fundamental rewards and trust (Huang et al., 2011). In sharing knowledge, social exchange arises when individuals co-operate in a knowledge sharing process. In this process, trust is significant and essential to sharing the knowledge (Lee et al., 2010; Disterer, 2001; White, 2001; Liebowitz, 1999). Trust is known as the utmost element in human communication, and therefore, it is the backbone of the knowledge sharing process in any organisation. Staff will work efficiently if they have the trust of others working with them (Safa et al., 2016; Lee et al., 2010; Roth & Broad, 2008; Hsu et al., 2007; Bos et al., 2002; Ridings et al., 2002; Jones & George, 1998).

Various empirical studies have supported the significance of trust when sharing knowledge in an organisation (Rutten et al., 2016; Safa et al., 2016; Hsu et al., 2007). Pan and Scarbrough (1998) argued that an atmosphere of trust is essential for knowledge sharing, as it is tightly linked to knowledge sharing (Lee et al., 2010; Scott Holste & Fields, 2010). Thus, the organisation must provide an atmosphere which supports staff to trust one another and where they are encouraged to knowledge share and participate in conversations. Such a type of atmosphere is necessary (see Table 2.14), as trust and sincerity could support vigorous knowledge sharing performance through successful communication promptness by providing a mandate to the members of organisations for sharing the knowledge that they possess (Pervaiz et al., 2016). In contrast, distrust can deter the emergence of a knowledge sharing process in any organisation (Willem & Buelens, 2009). In geographically spread organisations, electronic communication is considered to be an efficient source of connection, and it plays a vital role in information sharing.

Table 2.14 Need for trust in the knowledge sharing process

	Literature Findings	Source(s)
-	Trust of others is one of the main elements in the process of knowledge sharing.	Bălău and Utz (2016), Hashim and Tan (2015) and Usoro et al. (2007)
-	Social interchange is categorised by indeterminate personal responsibilities, fundamental rewards and trust.	Huang et al. (2011); Homans (1958)
-	In sharing knowledge, social exchange arises when individuals co-operate in a knowledge sharing process. In this process, trust is significant and essential to sharing knowledge.	Lee et al. (2010), Disterer (2001), White (2001) and Liebowitz (1999)
-	Trust is the backbone of a knowledge sharing process in any organisation. Staff will work efficiently if they have the trust of others working with them.	Safa et al. (2016), Roth and Broad (2008), Hsu et al. (2007), Bos et al. (2002), Ridings et al. (2002) and Jones and George (1998)
-	Various empirical studies have supported the importance of trust when sharing knowledge in an organisation.	Rutten et al. (2016), Safa et al. (2016) and Hsu et al. (2007)
-	An atmosphere of trust is essential for sharing knowledge.	Pan and Scarbrough (1998)
-	It is tightly linked to knowledge sharing.	Scott Holste and Fields (2010)
-	Trust and sincerity could support vigorous knowledge sharing performance through successful communication promptness by providing a mandate to the members of organisations for sharing the knowledge that they possess.	Pervaiz et al. (2016)
-	Distrust can deter the emergence of knowledge sharing in the organisation.	Willem and Buelens (2009)

Exclusive of trust, organisational distance and geographical position could become a psychosomatic limit to the process of knowledge sharing (Jones & George, 1998). Trust has a vital role in the knowledge sharing process (Bălău & Utz, 2016), so an untrusting environment is a major barrier to the knowledge sharing process (see Table 2.14) as it could cause the failure of organisational knowledge sharing processes for ID theft prevention in online retail organisations.

- **Fear of Information Leakage**

Information leakage fear is one of the barriers in the knowledge sharing process of ID theft in online retail organisations. The growth in the issues of the discourse of sensitive information has had considerable coverage in the media (Abecassis-Moedas & Rodrigues Pereira, 2016). Data leakage is becoming a main concern of online retail companies and, therefore, it has attracted the attention of researchers (Huth et al., 2013). For example, Farahmand and Spafford (2013) emphasised various significant aspects of data leakage, which included insiders (who leak valuable information).

Table 2.15 Fear of information leakage

Literature Findings	Source(s)
- The growth in the issue of disclosure of sensitive information has had considerable coverage in the media and by researchers.	Abecassis-Moedas and Rodrigues Pereira (2016)
- Research studies have emphasised various significant aspects of data leakage, which included insiders (who leak valuable information).	Huth et al. (2013) and Farahmand and Spafford (2013)
- The leak of profound information through undisclosed channels is a huge problem to manage in organisations. - Therefore, information leakage is becoming a main concern for online retail companies.	Marabelli and Newell (2012), Trkman and Desouza (2012), Desouza (2006) and Desouza and Vanapalli (2005)

The leakage of profound information through undisclosed channels is a challenging problem to manage in organisations (Marabelli & Newell, 2012; Trkman & Desouza, 2012; Desouza, 2006; Desouza & Vanapalli, 2005). This issue is intensified by the massive adoption of boundary-spanning (ITs), for example, cloud computing, networking technologies, social media and mobile devices.

Table 2.15 shows that securing information is necessary for organisations and fear of leakage of information is a barrier to knowledge sharing. Leakage of information can have various impacts on organisations, which include loss of revenue, reputational damage, loss of productivity, and costs arising from breaches of agreements of confidentiality in the organisations. With an extensive compensation struggle, the organisations can convalesce from such problems. However, employees working in the organisation have a fear of information leakage while sharing it with others, and therefore they are reluctant to share information security knowledge, especially the knowledge for ID theft prevention. As a result, it causes them to not share knowledge in the organisation and is one of the knowledge sharing barriers which need to be removed for an efficient process of knowledge sharing in organisations.

- **Insufficient Information Sourcing Opportunities and Inefficient ICT Infrastructure**

An effective knowledge sharing process requires well-structured information sourcing opportunities and a good IT infrastructure in any organisation. It is important for organisations to considering information as a resource in the organisation (Holsapple, 2013). Consequential procedures of making organisational learning or knowledge obtainable by expediting knowledge sharing among the skilled workforce are inevitable (Bhatt et al., 2010; Khan et al., 2016). Information sourcing opportunities or the ease of

gaining information is vital in the knowledge sharing process for ID theft prevention among individual staff members and teams. Consistent contact or communication networks to access expert information or the degree of technical and professional knowledge is easily obtainable and available by individuals and are examples of information sourcing opportunities. So there is a critical role of an ICT infrastructure for effective knowledge sharing for ID theft prevention.

Table 2.16 Need for information sourcing opportunities and effective ICT infrastructure in knowledge sharing

Literature Findings	Source(s)
- IT resources and the substantial procedures of making organisational learning or knowledge available by expediting knowledge sharing among the skilled workforce.	Bhatt et al. (2010) and Khan et al. (2016)
- The KM technology infrastructure includes the elements: intranet, communication networks, emails, data warehousing, and the decision support system. It is necessary for knowledge sharing in the organisation.	Stankosky (2005)
- Includes the technologies such as the internet, intranets, groupware which connect organisations to intra-organisational and inter-organisational level, and throughout the world	Holsapple (2013) and Martin (2000)
- Technology is known to be the main factor in implementing a successful KM program and the approach. An ICT infrastructure helps the employees to produce, store and share the knowledge with individuals, teams and departments. - A weaker IT infrastructure could fail the knowledge sharing process in the organisation.	Syed-Ikhsan and Rowland (2004)

The ICT technology infrastructure includes the elements: intranet, communication networks, emails, data warehousing, and the decision support system (Stankosky, 2005). The technologies which have been developed by keeping KM in mind comprise document management and workflow systems, innovative knowledge bases, and the expert systems applied in creating a collective memory, data filtering and data extraction systems. It also includes the technologies, for example, the internet, intranets, groupware which connects organisations to intra-organisational and inter-organisational level, and throughout the globe (Holsapple, 2013; Martin, 2000).

Table 2.16 shows that technology is considered to be the major element of implementing an affluent KM program and approach. It is known as an efficient source of generating, storing, and sharing knowledge. ICT infrastructure refers to effective KM based on people sharing their knowledge through computer facilities that users throughout the organisation have access to. In the organisation, an updated Information and

Communication Technologies infrastructure helps the employees to generate, store and share knowledge with individual employees, teams and departments (Syed-Ikhsan & Rowland, 2004).

Table 2.16 summarises the findings of the importance of knowledge sourcing opportunities and the IT infrastructure required for sharing knowledge in any organisation. The literature shows that these are vital in the process of knowledge sharing. Insufficient opportunities for information sources and an ineffective IT infrastructure are barriers in the process of knowledge sharing and need to be managed properly.

- **Lack of Leadership Support in Knowledge Sharing**

Leadership has a major role in managing the knowledge sharing process in any organisation (Muethel & Hoegl, 2016; Bass & Stogdill, 1990), as it is accountable for practicing strategic planning for effective use of the means and promotion of a learning culture and knowledge sharing (Boerner et al., 2007), along with the leadership required to bring about an unrestricted culture and to build an environment for knowledge sharing (Chuang et al., 2016). Furthermore, top management should provide support to promote the importance of knowledge sharing, providing needed support to those signifying knowledge sharing approaches (Mittal & Rajib, 2015).

Table 2.17 Need for support of leadership in the process of knowledge sharing

	Literature Findings	Source(s)
-	Leadership has an important role in managing the knowledge sharing process in any organisation.	Muethel and Hoegl (2016) and Bass and Stogdill (1990)
-	Leadership is accountable for practising strategic planning for efficient use of means and promoting learning culture and knowledge sharing.	Boerner et al. (2007)
-	Leadership is required to bring about an unrestricted culture and to build an environment for knowledge sharing.	Chuang et al. (2016)
-	Top management must provide support to promote the significance of knowledge sharing providing needed support to those signifying knowledge sharing approaches.	Mittal and Rajib (2015)
-	Senior executives and other management are required to reveal the distribution of their knowledge and use the knowledge of others in taking their actions and provide rewards to those who share their knowledge.	Aga et al. (2016) and Barnes (2001)

Importantly, senior executives and top management need to reveal the distribution of the knowledge, and use the knowledge of other persons when taking their actions (Aga et al., 2016), and provide rewards for those who share their knowledge (Barnes, 2001).

The literature clarifies that leadership plays a significant role in managing the knowledge sharing processes in any organisation. A lack of leadership support is an obstacle towards a knowledge sharing environment in an organisation (see Table 2.17). Not sharing knowledge could be the cause of ID theft in an organisation.

- **Weak Knowledge Sharing Culture**

Knowledge sharing refers to the sharing of awareness among individuals and between different teams and departments inside an organisation and various organisations. Organisational culture relates to the shared values, beliefs and performances of persons within an organisation (McDermott & O'Dell, 2001), and is one of the main elements considered in any organisation for information and knowledge sharing among individuals as well as teams inside the organisation (see Table 2.18). It is the most important element that needs to be understood in advance before employing any new strategies in the organisation (Syed-Ikhsan & Rowland, 2004). Furthermore, it is considered to be a significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM.

Table 2.18 Need for enhanced knowledge sharing culture in an organisation

Literature Findings	Source(s)
- Organisational culture refers to the shared values, beliefs and performances of persons within an organisation.	McDermott and O'Dell (2001)
- Organisational culture is one of the main elements considered in the organisation for knowledge sharing among individuals as well as teams. - It is the most important factor that needs to be understood in advance before employing any new strategies in the organisation.	Syed-Ikhsan and Rowland (2004)
- Culture is considered to be a significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM. - The knowledge sharing can work if the culture of the organisation supports it.	Stoddart (2001)

According to Stoddart (2001), knowledge sharing can work if the culture of the organisation supports it, but changes need to be developed according to the culture of the organisation, as having a weak culture of knowledge sharing causes hurdles to the knowledge sharing process (see Table 2.18). Therefore, it needs to be managed for an effective knowledge sharing process in the organisation.

- **No Job Rotation**

Knowledge sharing among individual staff members is concerned with how to establish communication among workers inside an organisation (Santos et al., 2016). Job rotation plays a major role in enhancing the knowledge of individual employees and teams within and outside any department in an organisation (Aga et al., 2016; Huang & Pan, 2014; Ortega, 2001).

According to Eriksson and Ortega (2006), there are three reasons for adopting a job rotation process in any organisation. One is *employee learning*, which makes the staff more efficient and resourceful. The second is *employer learning;* from the job rotation of employees, employers learn about the weaknesses and strengths of individuals working in the organisation. The third is *employee motivation*, which motivates the staff when working in a new environment and for new employees in the company. It therefore decreases the boredom of individuals and motivates individuals to learn new things. The literature shows that job rotation enables individuals to learn from various branches, decreases employee exhaustion caused by tedious or boring job tasks, and increases both individuals' confidence and the satisfaction in the job (Eriksson & Ortega, 2006; Kampkötter et al., 2016; Huang et al., 2005; Triggs & King, 2000). Job rotation plays a major role in enhancing the knowledge of staff members for ID theft prevention and sharing the knowledge of ID theft prevention (Kane et al., 2005).

Table 2.19 Need for job rotation in knowledge sharing

Literature Findings	Source(s)
- Knowledge sharing among individuals is concerned with how to establish communication among workers inside the organisation. - Job rotation plays a major role in enhancing the knowledge of employees. - Therefore, job rotation plays a vital role in enhancing the knowledge of individuals and teams within and outside any department in the organisation.	Santos et al. (2016), Aga et al. (2016), Huang and Pan (2014), Kane et al. (2005) and Ortega (2001)
- Employee learning, employer learning and employee motivation are the advantages of job rotation in any organisation.	Eriksson and Ortega (2006)
- Job rotation enables individuals to learn from various departments, decreases employee exhaustion caused by tedious or boring job tasks and increases both individuals' confidence and the satisfaction in the job.	Kampkötter et al. (2016), Eriksson and Ortega (2006), Huang et al. (2005) and Triggs and King (2000)

Table 2.19 shows that job rotation increases the knowledge of individuals, and enables employers to find out the employee's strengths and weaknesses. Therefore, a lack of job rotation causes the lack of enhancement of knowledge of individual staff members and teams in the organisation. Not rotating jobs leaves the individual staff to learn from their experience and is a barrier to knowledge sharing for ID theft prevention in an organisation. Therefore, it is important to implement the process of job rotation.

The literature clarified that staff unwillingness, lack of individual staff unawareness, insufficient learning opportunities, distrust of other staff members, a fear of information leakage, insufficient information sourcing opportunities and inefficient ICT infrastructure, lack of leadership support, a weak knowledge sharing culture, and no job rotation are major barriers in the processes of knowledge sharing for ID theft prevention. These barriers affect an adequate knowledge sharing process for ID theft prevention in online retail organisations. Therefore, this study included an investigation into existing barriers in knowledge sharing for ID theft prevention in online retail organisations as the third objective of the research study.

2.6. Need for Empirical Study on Knowledge Sharing for ID Theft Prevention in Online Retail Organisations

Personal information protection is one of the most critical issues while distributing the information of individuals and organisations (Abdullah et al*.,* 2016). The research on privacy protection comes from various areas, such as the retail industry, the banking sector, government and non-government organisations, educational institutions, health and insurance (Chen et al*.,* 2009). Due to improved consciousness and media reports on ID theft such as the theft of bank account details, credit or debit card information and other valuable personal information, products and organisations have intensified the interest and attention of people, organisations, governments and researchers (Shaobo Ji et al*.*, 2007).

In 2011, Shah and Okeke proposed a framework for the prevention of ID theft in the retail industry, identifying the engrossment of workers in ID theft criminalities within the industry. For the identification and prevention of ID theft related crimes they proposed a framework entitled *"Role Based Framework",* but the framework did not focus on knowledge sharing for ID theft prevention. Aimeur and Schonfeld (2011) proposed a

framework to detect ID theft related delinquencies by using computers, pointing out the information that hackers can share, possible attacks that can be performed and the places where required valuable information can be found. Kolaczek (2009) presented a method based on the analysis of social networks for the identification of ID theft related events. Similarly, other activities can be examined by studying the patterns of variation of observed activities on social networks.

Various organisations and government institutions have implemented different policies and standards to stop ID fraud. However, the rate of ID crimes is still increasing (Bush, 2016) due to the explicit nature of knowledge sharing in the form of policies and standards. Most workers do not follow the policies or do not even read policy and security related documents (Aimeur & Schonfeld, 2011). These issues can be dealt with by proper use of knowledge sharing within organisations (Conrad et al., 2012). Knowledge sharing and its importance are discussed in detail earlier in this chapter. This section discusses the requirement of knowledge sharing for ID theft prevention.

As discussed earlier, researchers have focused on knowledge sharing in different areas of rapidly growing industries such as e-marketing, telemarketing, e-banking, project management, e-commerce and other related areas. Liu Lihua et al. (2010) investigated the influence of knowledge in the products and the knowledge receiver's expertise on electronic commerce based consumer buying decisions. I-Ching Hsu et al. (2011) produced a platform of knowledge sharing based on web feeds for the project management team with knowledge acquired from different natured and distributed resources, such as web blogs, social network bookmarks and web-based multimedia.

One of the major concepts of knowledge sharing is tacit knowledge sharing (see Section 2.4). Tacit knowledge is the knowledge gained by doing things and experiencing them (Guang-bin et al., 2010). Salleh (2010) developed a model for sharing tacit knowledge in a public sector accounting organisation. The model connects the knowledge holder's process of sharing within accounting organisations.

The literature shows that, to some extent, work has been done on knowledge sharing, ID theft identification and prevention. Various surveys and case studies (Bush, 2016; Reyns & Henson, 2015; CIFAS, 2013; Reyns, 2013; Stephen Harrison, 2013; Bindra et al., 2012; Lai et al., 2012; Sakharova, 2012; Romanosky et al., 2011) have been conducted to understand ID theft. How big a problem is it for individuals as well as for organisations? The literature describes what the different categories of ID theft are and what various

frauds and crimes ID thieves are committing (Reyns & Henson, 2015; Fire et al., 2014; Bose & Leung, 2013; Reyns, 2013; Lai et al., 2012; Sakharova, 2012; Jin et al., 2011; Bilge et al., 2009;), and furthermore, the different methods of committing ID related frauds. The literature also adds the importance of knowledge sharing within organisations.

However, from the extensive literature review of knowledge sharing and ID theft, the researcher could not find the concept of knowledge sharing for ID theft prevention, such as where tacit knowledge sharing had been applied in an ID theft prevention context. Various organisations and government institutions, such as CIFAS and the UK police, have implemented different policies and standards to combat ID fraud (CIFAS 2017; Tony, 2013), but the rate of ID theft crimes is increasing (Aimeur & Schonfeld, 2011). Aimeur and Schonfeld (2011) claimed that employees typically do not adopt such policies, or even read the policy and security related documents.

Therefore, knowledge sharing for ID theft prevention is still not fully effective, and employees are still not fully concentrating on ID theft prevention. Due to this, personal information is still being stolen so organisations are not fully capable of protecting their valuable information and the information of related persons. Organisations are being victimised and bear significant financial losses due to the fraudsters. Therefore, research was required to investigate knowledge sharing processes for ID theft prevention in online retail organisations.

2.7. Theoretical Background of this Research

The last two decades have seen an enhanced awareness in KM by companies in various sectors and educational intuitions (Anumba et al., 2008). Via an enhanced interest in KM, different schools of thought have emerged. An extensive body of literature reports the KM from a diversity of schools of thought, and numerous research projects have been commenced which focus on several aspects of KM. According to Poynder (1998) and Bollinger and Smith (2001), there are three major schools of thought on KM. The first school of thought proposes that KM is an information technology issue (Al-Ghassani et al., 2004; Al-Ghassani et al., 2001). According to the second school of thought, KM is more of a human resource issue (Dainty et al., 2005; Olomolaiye & Egbu, 2004; Yahya

& Wee-Keat Goh, 2002). The third school of thought encourages the combination of both information technology and human resource perceptions (Bhatt, 2001).

According to the first school of thought, KM is an IT issue of computers, computer networks and groupware (Mason & Pauleen, 2003). Michael (2001) states it is a *"technocratic school of thought"* that emphases management technologies or information management to support employees in improving their performance in the business. According to that viewpoint, KM is a matter of information storing and retrieval via computers. The emergence of the internet, internal networks and ICT has enabled businesses to use a new set of tools for creating, coding and sharing knowledge. This school of thought supports the management of explicit knowledge (Stahle, 1999). Unluckily, those initiatives have resulted in failure (Fernie et al., 2003). Storey and Barnett (2000) investigated the study of failure for KM ingenuities, which established the role of human factors, perceiving that these failures were based on identification which recognised that KM is 90% human action and only 10% technology (Egbu, 2000).

Due to these reasons, KM has moved to the second school of thought, suggesting that KM is a human resource matter highlighting the culture of the organisation and teamwork in the organisation. Michael (2001) defines it in the words of *"the economic school"*, which considers knowledge to be an intellectual resource or asset to be oppressed. KM provides significance to the way in which people create and use knowledge, and identifies that learning and doing is much more critical to the success of a business than distribution and imitation.

A robust, optimistic organisational culture is a difficult place to enhance learning and increase the distribution of skills, resources and knowledge; additionally, the construction of societies of practice (Gillian Ragsdell et al., 2016; Wenger, 1998) and the improvement of social networks by which tacit knowledge is shared can be accomplished (Rice & Rice, 2005). It states that technology does not enable KM to work, but it is the procedure and atmosphere that matters (Mason & Pauleen, 2003; Gupta & Govindarajan, 2000). This school of thought enables the organisation to work amenably with people-centered co-ordination and includes the management of tacit knowledge (Stahle, 1999).

The third school of thought is known as the *'behavioural school'*, which undertakes the creation of a business culture that encourages knowledge creation, sharing, and its use (Michael, 2001). The processes are not essentially required to include the use of information technology; for example, work procedures (Davenport et al., 1996; Nonaka,

1994) as a means to manage the formation and/or communication of reasonably unstructured knowledge.

It is a combined perception which acknowledges that human resources and information technology standpoints complement each other (Preston et al*.,* 1999). However, the definition of KM is *"the process of creating, obtaining, apprehending, sharing knowledge"*. Wherever it exists, to increase the learning and performance in businesses (Preston et al*.,* 1999), it stresses both viewpoints. It is increasingly considered that an integrated approach of the behavioural school gives the highest chance of providing real benefits (Anumba et al*.,* 2008; Al-Ghassani et al*.*, 2005; Jashapara, 2004; Lee & Choi, 2003). Jashapara (2004) and Lee and Choi (2003) stated that efficient KM involves a relationship between the explicit and tacit knowledge together with both human resource practices and technology. Jashapara (2004) defined KM as *"the efficient process of learning linked to the exploration, exploitation and sharing of human knowledge which uses suitable technology and cultural environments for upholding the organisational intellectual capital and performance"*.

Therefore, the integrated approach was raised as being more appropriate for the current study as it provided the nature of the problems which have been investigated. Therefore, this study argued that both human resources and the IT viewpoints needed to be incorporated for an effective balance of knowledge sharing. Thus, the researcher selected the theory of KM for this study. Various frameworks have been investigated from the knowledge sharing and ID theft prevention perspectives (see Chapter 3). Following the comparison and contrasting of a knowledge sharing model proposed by Salleh (2010), this was selected as the guiding framework for extension in this study. Further details on the framework extension are discussed in the next chapter (Chapter 3).

2.8. Research Gaps in Existing Literature

The retail industry is plagued by ID theft. The major challenges associated with ID theft related offences include problems of consumers with credit, such as aggravation by debt collectors, rejections of loans, disturbance in normal lives such as reputation damage, and the psychological disruption of providing personal data to organisations and banks during the investigation (Shah & Okeke, 2011).

The literature shows that, to some extent, work has been done on knowledge sharing, ID theft identification and prevention. Various surveys and case studies (e.g. Reyns & Henson, 2015; Fire et al., 2014; Bose & Leung, 2013; Reyns, 2013; Lai et al., 2012; Sakharova, 2012; Jin et al., 2011; Bilge et al., 2009) have been conducted to understand ID theft, and how a big problem it is for individuals as well as for organisations.

The literature describes what the different categories of ID theft are and what various frauds and crimes are being committed by ID thieves, such as Bose and Leung (2013), Fire, Goldschmidt et al. (2014), Reyns (2013), Lai et al. (2012), Sakharova (2012), Jin et al. (2011), Bilge, Strufe et al. (2009), and the different methods used to commit ID related frauds. The literature also adds the importance of knowledge sharing within organisations. However, the literature review of this study could not find any examples of research undertaken so far where knowledge sharing concepts such as tacit knowledge sharing have been applied in an ID theft prevention context.

From the review of the existing area of study, the researcher found the following research gaps:

- Investigation of knowledge sharing processes for ID theft prevention in online retail organisations;
- Investigation of managerial practices to prevent ID theft in the organisations;
- Impact of knowledge sharing for ID theft prevention on employees in an organisation;
- Evaluation of knowledge sharing tools used for knowledge sharing for ID theft prevention in an organisation.

Knowledge sharing for ID theft prevention is still not fully effective, and employees are still not fully focussed on ID theft prevention awareness. As a result, personal information is being stolen, and companies are not capable of protecting their valuable information and the information of related persons; they are being victimised and suffering from huge financial losses caused by ID theft.

For these reasons and with the ready access of ID thieves to the online retail industry, this research studied, analysed and extended a framework for an enhanced knowledge sharing process for ID theft prevention in online retail organisations. This research study was an attempt to bridge that knowledge gap and provides a useful and novel contribution in this area of research.

2.9. Chapter Summary

The literature review chapter focused on ID theft describing what ID theft is, and how big a problem it is for the industry, as well as for organisations and governments throughout the world. The background of ID theft was discussed including different survey reports and research work undertaken in the area of ID theft awareness and prevention; for example, finding out at what level ID theft has been committed over the last few decades. Previous literature reviews found that a huge number of people had been victimised, the different methods of committing ID related frauds, the number of different ID related frauds recorded in various databases of security organisations throughout the world, along with the total number of frauds recorded in the United Kingdom, and which ID related frauds were the highest in the United Kingdom. Furthermore, it discussed different methods of committing ID related frauds. ID theft is divided into seven main categories, such as Financial ID Theft, Criminal ID Theft, ID Cloning, Commercial ID Theft, Medical ID Theft, opening new accounts and account takeover. Different types of ID theft frauds were covered, such as victimising individuals as well as organisations and the impact of these frauds on people and organisations. Several methods were developed and used for ID theft prevention in the existing literature.

The literature review also included KM and its importance and role in various organisations, including knowledge processing and knowledge sharing, focussing on how knowledge is being shared, the importance of knowledge sharing, what explicit knowledge sharing is, what tacit knowledge sharing is, and the difference between explicit knowledge sharing and tacit knowledge sharing and the research work that has been done in the field of knowledge sharing. It also included existing knowledge sharing approaches along with the challenges of setting up and implementing these difficulties. The significance of knowledge exchange in the performance of organisations and the factors impacting on knowledge sharing in organisations were also covered, as well as the role of individuals and teams in sharing knowledge for ID theft prevention in organisations. The literature review also included the need for managing existing barriers in knowledge sharing for ID theft prevention.

As to the role of knowledge sharing in the field of information security, during the literature review the researcher found that information security knowledge sharing was important for organisations. The review included how information security knowledge is

being shared within organisations, and how individuals, different teams and departments share information security knowledge inside organisations.

The need for an empirical study for knowledge sharing for ID theft prevention is covered in this chapter. It describes the role of knowledge sharing for ID theft prevention, how individuals share knowledge for ID theft prevention, and how different teams and departments share knowledge for ID theft prevention within organisations. This chapter also includes the theoretical development of this study. By the refinement of existing research, the researcher found the theory of KM appropriate to be used for this study.

Finally, existing research gaps are given after reviewing the literature in the area of knowledge sharing, information security, and ID theft prevention. Furthermore, one of those research gaps has been found to bridge the research gap in the existing area.

CHAPTER 3 THEORETICAL FRAMEWORK FOR THIS RESEARCH

3.1. Introduction

This chapter is about the framework development of this study. At the start, it includes the need for a framework of knowledge sharing for ID theft prevention in online retail organisations, and variously related frameworks from the area of knowledge sharing and ID theft prevention are included. A compare and contrast of existing frameworks is given for the selection of an appropriate framework for extension in the context of knowledge sharing for ID theft prevention. Criteria were set for the selection of a guiding framework of this research project, and an appropriate knowledge sharing framework proposed by Salleh (2010) was selected for extension in this study. After that, the structure for the guiding framework is discussed to produce the research themes.

3.2. Need for Framework of Knowledge Sharing for ID Theft Prevention in Online Retail Organisations

The knowledge sharing framework should be extended by ideas that affect a framework for sharing knowledge of ID theft prevention in a business organisation, depending on the clarity of the understanding and investigation of availability, and usage of existing known factors of knowledge sharing (see Figure 3.1). Knowledge sharing factors and their impact are discussed in Section 2.4.8 of the literature review chapter. For example, the technological tools used for sharing knowledge in an organisation, technical know-how and available training for knowledge sharing, knowledge sharing culture in the organisations, and leadership support for sharing knowledge for ID theft prevention (Islam et al., 2012; Martin et al., 2010; Salleh, 2010; Xu et al., 2006; Kim & Lee, 2004; Ives et al., 1997).

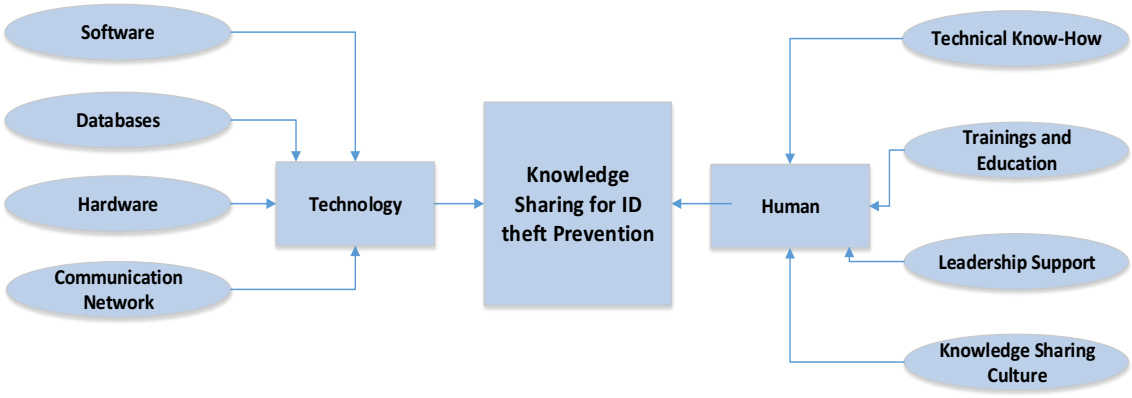

Figure 3.1 Organisational factors required for knowledge sharing processes for ID theft prevention

The chapter focuses on how individual members of staff share their knowledge for ID theft prevention in an organisation and investigates the knowledge sharing processes among the teams and departments within organisations. The theory of KM guided the analysis of the framework for knowledge sharing for ID theft prevention in the organisation. Understanding the theory of KM is provided in Section 2.7 of the literature review chapter. The next section includes the investigation of existing frameworks/modules from the area of knowledge sharing and ID theft prevention.

3.3. Investigation of Existing Frameworks in the Area of ID Theft Prevention and Knowledge Sharing

In this section, many existing knowledge sharing frameworks are briefly discussed, compared and contrasted, which led to the justification for the framework used for the extension and the central aim of this study. It includes the frameworks/models proposed and used in the area of knowledge sharing and ID theft prevention literature. Furthermore, their limitations are also discussed.

- **The Arachchilage et al. (2012) Framework**

Arachchilage et al. (2012) designed a framework to develop the conceptual knowledge to fight against phishing threats by raising awareness of the various phishing web addresses and emails to users. They also presented a prototype game design to educate users to prevent phishing.

- **The Trkman and Desouza (2012) Framework**

Trkman and Desouza (2012) developed an investigative framework which classifies knowledge sharing threats across various dimensions. The framework is a structured approach to knowledge threat management and counteracts the practice-based approach to knowledge risk management which was presented by Marabelli & Newell (2012). The framework outlines different types of known threats that organisations face. Trkman and Desouza (2012) used knowledge-based and transaction cost theories in conjunction to show how knowledge risk affects knowledge sharing among entities in the network, the entire network, and the risk alleviation options.

- **The Yan Li and Zetian Fu (2007) Framework**

Yan Li and Zetian Fu (2007) proposed a framework for the development of an expert knowledge sharing process system. The framework contains a collaborative sharing process for knowledge acquirement, depiction, assimilation and distribution, and an effective knowledge transformation and generation process for tacit and explicit knowledge. The framework is helpful for the project management team in the identification of primary value-adding activities into the software and system development. It was used for structuring the consideration and the evaluation of KM ingenuities. For research purposes, this framework could be utilised as a conjunction between strategies related to managing knowledge and operations in the development of an expert system.

There are two main limitations with this framework: one is that the knowledge generation and conversion process was not fully integrated into the flow chart, as it was illustrated on a separated basis; the second is that the framework did not determine the knowledge connections between the actors in a team undertaking similar tasks.

- **The Amin et al. (2010) Framework**

Amin et al. (2010) proposed a framework of internal and external influences of knowledge sharing to overcome the literature of the related area of research by re-examining the effect of extrinsic rewards and organisational citizenship behaviours in knowledge sharing. The proposed framework combined intrinsic Organisation Citizenship Behaviour and extrinsic rewards (motivators) in the Theory of Reasoned Action. The researchers tested 15 hypotheses, five of which were major.

The data was collected from the knowledge personnel, who were working as facilitators and trainers from three training institutes of an oil and gas company, using the questionnaire method. Amin et al. (2010) recommended, from the results, that the influence of extrinsic plunders is moderate in knowledge sharing. Therefore, organisations cannot rely solely on extrinsic rewards to motivate persons to share their knowledge. Organisation citizenship behaviour is an adamant prognosticator of knowledge sharing behaviour and, therefore, organisation citizenship behaviour should be inculcated in the organisation for effective knowledge sharing in organisations.

The proposed framework has limitations as data was collected from the training institutes of one company, as results may vary in different organisations and various departments in organisations, and another limitation was that the research approach adopted could be biased by the responses of peers.

- **The WenJie Wang et al. (2006) Framework**

WenJie Wang et al. (2006) proposed a framework for identifying stakeholders and the communicating connections which play various roles in ID theft prevention. In the framework, ID owners, ID issuers, ID protectors and ID checkers were considered to be the four main stakeholders to help with the prevention of ID theft through different detection, prevention, legitimate fortification and theft prosecution activities.

The WenJie Wang et al. (2006) framework indicates some research directions but does not provide any specific solutions to prevent ID theft, as well as not focusing on knowledge sharing for ID theft prevention; but it identifies some connections which could be helpful for ID theft prevention due to the fact that this framework relates to this research.

- **The Noor and Salim (2012) Framework**

Noor and Salim (2012) proposed a conceptual framework which contains the effect of individual, organisational and technological aspects of knowledge sharing inventiveness, so that top level management who are interested in developing and nourishing knowledge sharing in the organisation must focus on the three most important factors. The authors used qualitative and quantitative methods for research and data was collected from private sector organisations in Malaysia.

The scope of their research is limited as the authors collected data from a private organisation; the results could have been different if data had been collected from public

sector organisations which have various parameters as per the nature of the organisations. Furthermore, the proposed framework focused on enhancing organisational performance rather than having an emphasis on knowledge sharing for ID theft prevention.

- **The Salleh (2010) Framework**

Salleh (2010) proposed a knowledge sharing model that connects KM implementers and the process of sharing tacit knowledge in a public sector accounting organisation. The proposed relationship model interconnects solutions of KM through culture, leadership, learning and technology to enhance the knowledge sharing process in the organisation. The knowledge sharing model enables the tacit knowledge sharing process and is useful as a process of strategic KM which supports knowledge networks and knowledge flow to enhance the decision-making process in the organisations.

This framework could be extended for knowledge sharing for ID theft prevention inside an organisation, as it supports the understanding and management of most of the attributes of this research, such as information and communication technologies knowledge and skill of the individuals, information and communication technologies infrastructure and software, KM technologies available, job training, rotation of jobs, feedback on the basis of performance evaluation, learning opportunities available, opportunities for sourcing information, support of leadership, and a culture of knowledge sharing. The researcher also investigated other related frameworks.

Various frameworks and models have been developed to understand the knowledge sharing process inside organisations. Szulanski (2000) developed a model having four stages: origination of transference, starting enactment, ramp up to acceptable performance, and integration, which needed follow-through and estimation for the integration or transformation of the new practices into the past practices of the knowledge receiver. Goh (2002) developed an integrative framework that added the main factors, having a significant impact on the effective dissemination of knowledge, assuming that knowledge sharing needs a cooperative and collaborative culture.

Table 3.1 Frameworks for knowledge sharing v/s ID theft prevention

Framework / Model	Description	Knowledge Sharing	ID Theft Prevention
Arachchilage et al. (2012) Framework	The framework proposed to develop conceptual knowledge to fight against phishing threats by giving awareness about various phishing web addresses and emails to the users.	Yes	Yes
Trkman and Desouza (2012) Framework	An investigative framework that classifies knowledge sharing threats across various dimensions. The framework outlines different types of known threats that organisations face.	Yes	___
Yan Li and Zetian Fu (2007) Framework	The framework was developed for a knowledge sharing process expert system development. It contains a collaborative sharing process for knowledge acquirement, depiction, assimilation and distribution, and an effective knowledge transformation and generation process for tacit and explicit knowledge.	Yes	___
Amin et al. (2010) Framework	The framework was developed to understand internal and external influences of knowledge sharing to overcome the literature of the related area of research by re-examining the effect of extrinsic rewards and organisational citizenship behaviours in knowledge sharing.	Yes	___
WenJie Wang et al. (2006) Framework	The framework proposed identifying stakeholders and the communicating connections which play various roles in ID theft prevention. In the framework ID owners, ID issuers, ID protectors and ID checkers were considered to be the four top stakeholders to help in the prevention of ID theft through different detection, prevention and legitimate fortification and theft prosecution activities.	___	Yes
Noor and Salim (2012) Framework	A conceptual framework which comprised the effects of individual, organisational and technological aspects of knowledge sharing inventiveness, so that top level management interested in developing and nourishing knowledge sharing in an organisation must focus on the three most important aspects.	Yes	___
Salleh (2010) Framework	Knowledge sharing model that connects KM implementers and the process to share tacit knowledge in accounting in a public-sector organisation. The proposed relationship model interconnects solutions of KM through culture, leadership, learning and technology to enhance the knowledge sharing process in the organisation.	Yes	___

Interface problems have been considered while sharing knowledge between organisations, and due to that, several models have been developed, such as Abou-Zeid,

(2005), Mohr & Sengupta (2002), and Agrawal (2001). Abou-Zeid (2005) developed a conceptual model for inter-organisational knowledge sharing as a culturally aware four-step process containing initiation, inter-relations, implementation and internalisation, which provided a close investigation of how the cultural characteristics of senders and receivers of organisations at various stages impacted on each stage of the process. Chen et al. (2006) assumed that knowledge sharing in small and medium enterprises followed the process of having identification, cooperation, selection, collaboration and exchange stages.

Various knowledge sharing models were also addressed for communication and knowledge sharing between organisations at the world level. Schlegelmilch and Chini (2003) proposed a conceptual framework for efficient marketing and discussed the effects of organisational remoteness, cultural difference, tactical order and efficiency to involve knowledge sharing between multinational companies. Cummings and Teng (2003) incorporated intra- and inter-organisational knowledge sharing in which companies share their knowledge and gain the advantage of association for communication and processing. Miesing et al. (2007) developed a model which showed adequate intra-organisational knowledge sharing in different nations which needed the formation of social capital between the members and required a collaborative transitional approach.

Table 3.1 describes several related frameworks or models for this research.

The following criteria were set to evaluate the frameworks and select an appropriate framework for this study:

1. **Functionality:** the framework should be capable of fulfilling the research objectives/capable of functioning.
2. **Comprehensiveness:** it should cover the factors of knowledge sharing but should not be too complex.
3. **Adaptability:** the frameworks must be flexible and able to be modified for the purpose of this study (new purpose).
4. **Ongoing improvement:** it should focus on ongoing improvements, such as it should enable the sharing of knowledge within an organisation.
5. **Empirically derived:** it should be empirically derived from previous research.
6. **Focused components:** the framework should have components focusing on the research.

Table 3.2 shows the comparison of existing frameworks. The Arachchilage et al. (2012) framework was proposed for the development of conceptual knowledge for fighting against phishing threats on the internet, as it gives awareness about different phishing web addresses and emails to the internet users. The framework supported knowledge sharing and ID theft identification, but it could not be used in this research because this research is focused on how individuals, teams and departments share their knowledge for ID theft prevention inside retail industry organisations. The Trkman and Desouza (2012) framework classifies knowledge sharing threats across different dimensions and outlines various types of known threats that organisations face. The proposed framework is useful for knowledge sharing risk assessment and management, but it could not be used in this research as this research is for sharing knowledge for ID theft prevention.

Table 3.2 A comparison of related frameworks

Framework/Model	Functionality	Comprehensiveness	Adaptability	Focused Ongoing improvement	Empirically derived?	Focused components	
						Knowledge sharing	ID Theft Prevention
Arachchilage and Love et al. (2012)	No	No	N/A	No	Yes	Yes	Yes
Trkman and Desouza (2012)	No	Limited	N/A	No	Yes	Yes	No
Yan Li and Zetian Fu (2007)	No	Limited	N/A	N/A	Yes	Yes	No
Amin et al. (2010)	N/A	Limited	No	Limited	Yes	Yes	No
WenJie Wang et al. (2006)	N/A	N/A	N/A	No	No	No	Yes
Noor and Salim (2012)	Yes	Limited	No	Limited	Yes	Yes	No
Salleh (2010)	Yes	Yes	Yes	Yes	Yes	Yes	No

The Yan Li and Zetian Fu (2007) framework was developed for knowledge sharing process expert system development, which contains a collaborative sharing process for knowledge acquirement, depiction, assimilation and distribution, and is an effective knowledge transformation and generation process for tacit and explicit knowledge. This framework could not be used as it contains two main limitations: one is that the knowledge generation and conversion process was not fully integrated into the flow chart as it was illustrated on a separated basis; the second is that the framework did not determine the knowledge connections between the actors in a team for similar tasks.

Furthermore, it was not capable of use in a contest of knowledge sharing for ID theft prevention.

The Amin et al. (2010) framework was developed to understand the internal and external influences of knowledge sharing for overcoming the literature of the related area of research by re-examining the effects of extrinsic rewards and organisational citizenship behaviours in knowledge sharing. The proposed framework could not be trusted and used in this research because data were collected from training institutes of one company and results may vary in different organisations and various departments, and another limitation was that the research approach adopted could be biased in the response of peers.

The WenJie Wang et al. (2006) framework is used for identification of stakeholders and the communicating connections which play various roles in ID theft prevention. Though that framework was related to ID theft prevention as it identifies some connections which could be helpful for ID theft prevention, it did not contain the learning process for knowledge sharing for ID theft prevention. Due to that, the framework was not selected as the guiding framework.

The Noor and Salim (2012) framework comprised the effect of individual, organisational and technological aspects of knowledge sharing inventiveness, so that top level management interested in developing and nourishing knowledge sharing in the organisation must focus on the three most important aspects. The proposed framework focused on enhancing organisational performance rather than focusing on sharing knowledge for ID theft prevention. Therefore, this framework was not selected for use in this research.

3.4. Selection of Guiding Framework for this Study

After an extensive research and investigation of existing frameworks in the field of knowledge sharing and ID theft prevention, the knowledge sharing model proposed by Salleh (2010) was selected for extending the context of knowledge sharing for ID theft prevention. The following section describes the existing frameworks/models in the field of knowledge sharing and ID theft prevention.

The proposed framework connects KM implementers and the process to share tacit knowledge in a public-sector accounting organisation. The model interconnects solutions of KM through culture, leadership, learning and technology to enhance the knowledge

sharing process in an organisation. Figure 3.2 describes the conceptual model proposed by Salleh (2010), which has been used by Siong et al. (2011) for KM implementation in a public sector organisation. It enables the tacit knowledge sharing process and is useful as a process of strategic KM that supports knowledge networks and the flow of knowledge to improve the decision-making process in the organisations.

Figure 3.2 Conceptual framework proposed by Salleh (2010)

Individuals, as well as teams, play a major role in the success of organisations, so the staff of a successful organisation should be familiar with the use of existing information systems for knowledge sharing processes for ID theft prevention. The following elements of the guiding framework play the main role in enhancing the knowledge sharing processes for ID theft prevention.

- **ICT know-how and skills**

Information and Communication Technology (ICT) refers to information communication by using telecommunication systems. ICT infrastructure plays a vital role in knowledge sharing among the individuals within and outside the organisation. It is essential to know about the information and communication technology skills required in the organisations

to assess the ability of persons for use of those skills to solve complicated problems of information management, knowledge sharing and presentations (Cobo, 2013).

These problems should include both learning and technological skills, such as developing ideas, sharing information and finding things out (Cobo, 2013; Dede, 2010). To understand the tasks, employees require particular practical skills ('know-how') to perform the required tasks very well. These know-how skills can be learned and developed over time. This learning might be the result of the independent learning process or detecting and emulating others' skills, which are the approaches of tacit knowledge sharing for ID theft prevention within their organisation (Letmathe et al*.,* 2012).

- **Job Training**

Job training has a significant role in knowledge sharing to enhance people's knowledge. Job training can be divided into two categories: one is *General Training*, referring to the training which impacts on general human capital and enhances the productivity of work in all types of jobs, for example, training to enhance general computer skills and different language training courses, although the knowledge and general skills can be shared with job holders in similar firms, such as companies competing in the same industry sector, and to similar jobs in the same profession and skills; the second is *Firm-Specific Training*, which enhances knowledge only in the workplace in the current organisation. This training is provided to improve the knowledge about the machines, and understand the infrastructure of the workplace and procedures which are used only within the firm where the employee is working, which can be provided to gain knowledge about particular characteristics of the products and customers of the organisation or firm (De Grip & Sauermann, 2013).

- **Job Rotation**

Knowledge sharing among individuals is concerned with how to establish communication among workers inside the organisation. It is essential to know how to improve the exchange of expertise of knowledge holders among other persons in the organisation. The most significant issue concerns trust within the organisation, such as how willing are individuals to share what they know? To answer these questions leads to activities based on trust building, team creation, job rotation and so forth (Sveiby, 2001). Job rotation plays a major role in enhancing the knowledge of employees to prevent ID theft and sharing their knowledge for ID theft prevention (Kane et al*.,* 2005).

- **Feedback on Performance Evaluation**

Feedback is important for the assessment and measurement of activities of employees in the organisation. Companies have observed their workers for a long time; however, current developments in electronic technology are advancing the nature of monitoring the performance of employees (Alder & Ambrose, 2005).

Feedback can be given for various purposes, such as including the outcome of activities or processes, giving information when workers move away from primarily set goals, helping to establish new goals or adjust the real goals, or guidance to perform their activities. Furthermore, it promotes critical reflection on situations and tasks to bring about new approaches (Gabelica et al., 2012). It can be helpful to understand the knowledge level of staff for ID theft identification, ID theft prevention and sharing knowledge among other staff members.

- **Learning Opportunities**

A learning environment leads the organisation to the height of success and defines procedures leading to the accumulative capabilities and skills through routine work. It is a priority of many enterprises who consider themselves to be continuous learning organisations to enhance the potential of their workers for the sake of competitiveness in the global market. Learning opportunities enhance progress in outcomes by removing previous mistakes and weaknesses (Harteis et al., 2008).

An advanced learning environment facilitates the workers to enhance their expertise by increasing their knowledge to deal with complicated problems they may face. Many organisations provide various training opportunities for their employees to keep them up-to-date with processes of work and to enhance innovative techniques to perform the activities to increase their outcomes.

- **Information Sourcing Opportunities**

Brown and Starkey (1994) presented the perception of information awareness to be generated in the organisation, which relates to the attitude of an organisation to considering information as a source and the consequential procedures of building organisational learning or knowledge available through expediting knowledge sharing among the proficient workforce (Majewski et al., 2011). Information sourcing opportunities or ease of obtaining information is vital for knowledge sharing for ID theft prevention among individual employees and teams/groups. Consistent contact or a

communication network to retrieve the information or the degree of technical and professional knowledge is certainly obtainable and available to individuals who are examples of information sourcing opportunities.

- **KM Technologies**

The KM technology infrastructure includes the elements: intranet, communication networks, emails, data warehousing, and the decision support system (Stankosky, 2005). The technologies which have been developed by keeping KM in mind comprise document management and workflow systems, innovative knowledge bases, and expert systems applied to create a shared memory, data filtering and extraction systems. It also includes technologies. For example the internet, intranets, and groupware which connect organisations to intra-organisational and inter-organisational level and throughout the globe (Martin, 2000).

- **Leadership Support**

Leadership is accountable for practising strategic planning for efficient use and promoting a learning culture and knowledge sharing. The leadership is required to bring about an open culture and to build an environment for knowledge sharing. Furthermore, top management should offer the support to promote the importance of knowledge sharing and provide support to those signifying knowledge sharing approaches. Significantly, senior executives and top management need to reveal the distribution of their knowledge, use the knowledge of others in taking their actions, and provide rewards to those who share their knowledge (Barnes, 2001).

- **Knowledge Sharing Culture**

Knowledge sharing refers to the sharing of awareness among individuals, different teams, and departments inside an organisation and the various organisations. Organisational culture relates to the shared values, beliefs and performances of persons within organisations (McDermott & O'Dell, 2001). A knowledge sharing culture is one of the main elements considered in the organisation for information and knowledge sharing among individuals as well as teams inside an organisation. It is the most important factor that needs to be understood in advance before employing any new strategies in the organisation (Syed-Ikhsan & Rowland, 2004). Culture is considered to be a significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM. According to Stoddart (2001), knowledge

sharing can work if the culture of the organisation supports it, and the changes required are developed according to the culture of the organisation.

- **ICT Infrastructure and Software**

Technology is considered to be the main factor of implementing a prosperous KM program and approach. It is known to be an effective means of creating, storing, and sharing information. Information and communication technology infrastructure refers to an effective KM, which is based on people sharing their knowledge through computer facilities. In the organisation, an updated Information and Communication Technologies infrastructure helps the employees to generate, store and share knowledge with individuals, teams and departments (Syed-Ikhsan & Rowland, 2004).

The framework could be used for knowledge sharing processes for ID theft prevention inside the organisation. It contains most of the attributes which could be useful in this research, such as information and communication technologies knowledge, the skill of the individuals, information and communication technologies infrastructure and software, the KM technologies available, job training, rotation of jobs, feedback on the basis of performance evaluation, the learning opportunities available, opportunities for sourcing information, support of leadership, and a culture of knowledge sharing. Therefore, the model proposed by Salleh (2010) was selected to extend in the context of the knowledge sharing for ID theft prevention inside the retail industry organisations.

3.5. Research Themes of the Study

This study included thematic analysis, which was included to fulfil the requirements of the current research established on the contextual reading of the knowledge sharing framework. The important themes were adopted from the guiding framework (Salleh, 2010). This study created new themes to fulfil the requirements of the investigation and provided a framework of knowledge sharing for ID theft prevention in the organisations. The framework extension section of the discussion analysis chapter included all the themes known as knowledge enablers for knowledge sharing processes for ID theft prevention in an online retail organisation.

This study included the following research themes:

- ICT know-how and training;

- Information sourcing opportunities;
- Job rotation;
- Feedback on performance evaluation;
- Leadership support;
- Knowledge sharing culture;
- KM infrastructure.

3.6. Chapter Summary

This chapter included the development of the framework for this study, the importance of which was discussed at the start of the chapter. The researcher used the theory of KM in this study. The framework of knowledge sharing for ID theft prevention was based on technological and human perspectives, and the researcher set criteria for selection appropriate to guiding the framework for the extension of the present study. Via the scrutiny of various frameworks of knowledge sharing and ID theft prevention, an appropriate knowledge sharing framework proposed by Salleh (2010) was selected for extension in the context of knowledge sharing for ID theft prevention. Following this, the structure of the guiding framework was discussed, and important themes were borrowed from the guiding framework. New themes were created for the investigation of the current study and the extension of the framework.

CHAPTER 4 RESEARCH METHODS

4.1. Introduction

This chapter includes the philosophical approach, the adopted research strategy, and the research design of the current study. To answer the research questions posed in the first chapter of the thesis, the researcher gave consideration to various approaches of the philosophy and existing research methodologies used for adoption. Only those having relevance are reported in this chapter. The adoption of a philosophical perception emphasises the beliefs of the researcher for the nature of reality (ontology) and potential ways of obtaining the knowledge (epistemology).

The selection of the philosophical approach must necessarily be the first step in research, as according to Guba and Lincoln (1994), *"the questions of method are inferior to the issues of paradigm"*. Here, paradigm refers to the major philosophical assumption or belief system of the researcher, guiding the researcher to the selection of a suitable research method; it also mirrors the investigator's view around the nature of reality, and in what way knowledge is/should be gained.

Existing literature divides research methodology into two types: one is quantitative research methodology; the other is qualitative research methodology (Fremeth et al., 2016). Quantitative research methodology is commonly linked with 'positivist' philosophy and is concerned with quantification, replicability, objectivity and causality (Bryman, 1984). The use of huge volumes of data in quantitative research imparts itself to use statistical methods which are applied in analysing the results. The survey is the preferred instrument of inquiry in this practice (Rubin & Babbie, 2016), although experimentation and secondary analysis of data can also be used (Lovell & Rosenberg, 2016). Quantitative methods focus on facts instead of judgements.

The philosophical foundations of the qualitative methodology are often related to phenomenology and hermeneutics (Blaikie, 2007). In qualitative research, prominence is given to watching the social world from the opinion of the performers. Therefore, qualitative investigators attempt to develop a critical understanding of the problem under study by data collection in a real location where actors are involved in the problem (Creswell, 2014).

Each research approach has strengths and weaknesses. However, the choice of an appropriate research strategy depends on the type of investigation questions posed and the amount of control the researcher has on the research themes (Creswell & Clark, 2007). This research study used an interpretive approach, and the strategy was based on the use of case studies.

4.2. Philosophy of this Research

To indicate the assumptions of the researcher, and to justify the selected research strategy, the overview of the philosophical viewpoints is significant. Therefore, the researcher gave considered thought to the philosophical perceptions in social science research. The researcher found the two most important philosophical approaches in the social sciences research were positivism and interpretivism (Bryman, 2015; Hughes & Sharrock, 1997).

4.2.1. Positivism

What can be said as modern scientific rationale (Enlightenment period) has been endorsed by two prominent people, Francis Bacon (1561-1626) and René Descartes (1596-1650). In that period, the divine or theological descriptions of the world were forbidden in support of scientific enlightenment. Bacon was an empiricist who gave emphasis to the significance of straight observation of patterns in experiential data from which universal laws can be concluded as the basis of understanding (Mukherji, 2000). According to him, a genuine knowledge of nature required focus on the *'methodical accumulation of experientially tested findings'* (Hughes & Sharrock, 1997). Descartes, on the other hand, although not refuting the significance of direct observation, focused the part of knowledge produced rationally from human reasoning (Rationalism). It was the earlier part of the epistemological division which was the basis of the positivist philosophy (Hughes & Sharrock, 1997).

'Positivism' has been accredited to Auguste Comte as a term he introduced. Positivism has advanced over many years, hence the several versions (Bernard & Bernard, 2013; Hughes & Sharrock, 1997; Mukherji, 2000). These several versions can be gathered into the 1st generation positivists, the 2nd generation logical positivists, and the post 2nd world war positivists. Auguste Comte and other philosophers, for example, Locke and Hume, were related to the 1st generations of positivism. Auguste Comte pooled Francis Bacon's

notion of creating universal laws from general empirical observation (contradicting the rationalists' claim that knowledge could be produced from thought only), eventually prolonging this indication from the study of the natural world to the social world. For Auguste Comte, the social world was similar to the natural world, and henceforth society, including beliefs and values, could be investigated similarly to the natural world. By such a claim, Auguste Comte underplayed inimitable human factors, for example, free choice, will, emotions, etc. (Hughes & Sharrock, 1997). Auguste Comte's opinions were distributed and ultimately further spread by other philosophers, including Emile Durkheim (1858-1917) and John Stuart Mill (1806-1873).

Logical positivists of the Vienna Circle emphasised the significance of verification of laws or theories through using quantitative data in testing hypotheses derived from the theories. The theories are scientifically meaningful for the logical positivists only if they can be measured and confirmed empirically (by observation and/or measurement) (Bernard & Bernard, 2013; Hessler, 1992). Additionally, logical positivists consider that neither the research idea nor the scientific concept is so abstract that it cannot be observed or measured. If it is not measurable, then it does not signify objective realism and is not science, and therefore it is meaningless.

The 3rd version of positivism that dominated after the Second World War was related to developing explanations in the shape of universal laws (Blaikie, 2007). That type of positivism was produced from the 2nd version, and its main focus is that all sciences, including social sciences, are related to developing clarifications in the shape of universal laws or generalisations. Any phenomenon can be described by signifying that it is a particular case of some form of universal law (Blaikie, 2007).

Regardless of the version, the key is the impression that an objective reality occurs independently of human behaviour, and therefore is not a formation of the human mind. The comment of David Hume also captures the idea of positivism well:

> *"If we take in our hand any volume; of divinity or school metaphysics, for instance; let us ask, does it contain any abstract reasoning concerning quality or number? No. Does it contain any experimental reasoning concerning matter of fact and existence? No. Commit it then to the flames: for it contains nothing but sophistry and illusion."* (Hume, 1975 c.f. Hughes & Sharrock, 1997; p. 28)

Positivism is characterised by Blaikie (1993) as follows:

- Scientism - the scientific approach to investigation is common. Therefore it is effective for any research and discipline, including investing in social science.
- Nominalism - the scientific descriptions or the laws necessarily produced from sensual observation. Incorporeal concepts that are not possible to observe are not commendable of the named knowledge, and therefore may pass for mere names or words.
- Phenomenalism - only the observation or what the investigator can directly observe is the foundation for scientific knowledge; whatever cannot be directly observed, cannot be considered as knowledge.
- The purpose of science is to form scientific laws, to recognise original descriptions of natural phenomena.
- Value judgements - the positivist gives emphasis to a separation of the facts and the values, refusing values as having the position of knowledge since it cannot be discoverable by direct observation.

The other key ideas associated with positivism are also identified by Neuman (2011), for example:

- There is an exterior objective realism which is independent of human behaviour. Positivists consider a mechanical model of a human, which means that people respond to external factors (generating consequences, for example behaviour or attitudes), and in much the same way as objects react to physical forces. Therefore, a reason will have similar influence on everyone.
- Scientific knowledge is dissimilar from, and superior to, all other knowledge and only knowledge engaging a firmness, systematic and methodical approach to the disciplines can be the base for reality. Only the outcomes of employing a scientific (physics and astronomy) approach can be considered as knowledge (Bentz & Shapiro, 1998).
- There is a focus on authentication - replication confirms theories through investigators.
- It is the objective.
- Value freedom – the scientific reality must be commenced not dependent on political, religious, or personal beliefs of scientists. The science is capable of

operating independently of the beliefs of the researchers, due to the involvement of strict rational and systematic observation that transcends personal values and biases (Neuman, 2011).

Positivism also needs the investigator to undertake an unreceptive or unbiased role in the investigation procedure. In this logic, the researcher's basic purpose is to perceive facts or sensual data, without vigorously engaging with the inquiry subject (Bentz & Shapiro, 1998). Likewise, in the way that 'values' do not have a place in science, the investigator's context does not have to bear and would not enter into the investigation because situations or perspectives familiarise subjective and unreasonable features into the inquiry process. *'The world is a totality of facts without context'* (Ibid).

In the present study, concerning the sensitive nature of the research topic and the likelihood that companies may be cautious about revealing such information or their current strategies or measures to reduce such actions, particularly to an outsider, a level of trust that a permitted research contributes to matters had to be established openly. This meant that retaining a distance between the participant and the researcher was impossible. Qualitative methods are suitable for encouraging respondents, by initially being very careful in order to reduce their reservations, and starting with standardised or inflexible techniques, which questionnaires might not. When an investigator seeks individual opinions, a positivist philosophy is not the ideal approach.

Whereas positivist methodologies are scientifically rigorous, there are apprehensions that human behaviour might not be as anticipated by the positivist proponents (Blaikie, 1993; Bryman, 2015). As a result, standard or rigid methods which do not contemplate the inimitability of human behaviour may not give the flexibility of the method needed. Additionally, the quest for straight observable/measurable/quantifiable data might not generate the full complexity of the nuances in the study, as with a qualitative approach (Bryman, 1984; Kelle, 2006).

The criticisms of scientific or quantitative approaches to the inquiry of the social world provoked the attention in qualitative research capable of interpreting the actions of people and their social world from their viewpoint. The purpose of the present study was to investigate the knowledge sharing process for ID theft prevention in an organisation. It required eliciting the opinions and the actions of participants regarding knowledge sharing processes. Therefore, a positivist philosophical position was not adopted in this study.

4.2.2. Critical Realism

Critical realism is a comparatively new philosophical viewpoint related to Bhaskar (1978). The concept of Bhaskar emerged by connecting his general philosophy of science, which is also called transcendental realism, with critical naturalism, which is his philosophy of the social sciences. Where recognising that the scientific way of the physical sciences can be useful to the social world, Bhaskar claims that the dissimilarities in the problems of the physical and social world need a different method when applying the scientific method to the investigation of the social world.

Bhaskar claims that realism is entirely independent on our understanding of it as a reality, and our understanding of its function in different dominions, such as the transitive epistemological domain and the intransitive ontological domain (Bhaskar, 1978). This difference is the view of the universe that we cannot confidently understand (the so-called epistemic fallacy) since human knowledge is imperfect (Dobson, 2001; Guba & Lincoln, 1994). As a result, critical pragmatists consider that we can only be closer (which is never perfect) to catching realism and that claims for reality should be 'critically' inspected; the purpose is to emanate as close to a perfect (but never perfect) understanding of the reality (Guba & Lincoln, 1994).

Critical realism focuses on a stratified ontology including the empirical, the actual and the real domains of realism. The work of Bhaskar Blaikie (2007) records that:

> *'the empirical domain is included, the critical realism of occasions that can be perceived. The real is the domain of substantial presence, including events and things, whether they are observed or not. The real domain comprises processes or mechanisms (unobservable events) that create these occasions which are presumed to the act individualistically of the events they generate.'* (Blaikie, 2007)

As such, critical realism considers that there is realism 'out there' and that such a reality exists irrespective of whether it is observed or not. Therefore, the reality is grounded in the supposition that the empirical and the conceptual do not exhaust the real.

In this philosophical perception, experiments are done in closed atmospheres (such as the laboratory) where the connection between the cause (known as tendencies) and the influence is observed. Critical realism claims that the world outside the laboratory is an exposed social system consisting of a multitude of arrangements which form human

actors, and which are in turn converted and reproduced by them (Blaikie, 1993). By this, critical realists, in contrast to positivists, identify the importance of the meaning of creation and communication amongst human actors. However, at the same time, they highlight that previous social construction may impact on human activities. Hence, the social world can be understood if we comprehend both the understandings of human actors as well as revealing the more profound structures and mechanisms that condition human acts (Dobson, 2001). Specifically, it follows that the use of theories in open social systems is to explicate or describe, instead of predict, the social phenomena. This is different to the positivist view that the purpose of science is to generate scientific rules to predict the phenomena. So, the aim of realist investigation is to examine generative mechanisms instead of predictive theories.

The principles of realist ontology are summed up by Outhwaite (1987 c.f. Blaikie, 1993, p.61):

- The difference is made between the real entities (an intransitive domain), and the models, theories and concepts, (a transitive domain) which create the natural and social worlds.
- A stratification of reality into the real, the actual and the empirical domains.
- The concept of causal relations as tendencies or powers of the things which either interact or not with other tendencies to generate events.
- In the domain of reality, the real definitions are declarations about the simple nature of some objects.
- Enlightenment in the real domain includes the notion of mechanisms and an attempt to prove their presence.

This philosophical perspective is situated between the positivism and the interpretivism, in which critical realism, like positivism, considers that there is realism out there regardless of someone's interpretations of it. However, critical realism shares the view of interpretivism as social realism is pre-interpreted.

4.2.3. Constructivism

Since this research study aimed to investigate the knowledge transfer process for ID theft prevention in a retail organisation, it studies how individual staff members and teams share knowledge for ID theft prevention based on the interaction and behaviour of

individuals, groups and teams, and the researcher considered appropriate conception of constructivism. It is an ontological position that stresses that the social actors are repeatedly accomplishing social phenomena and their meanings. Furthermore, it denotes that social phenomena and categories are not only generated through social interactions but they are in a constant state of revision. For example, in some organisations rules are less extensive and less rigorously imposed than in other classic organisations.

Moreover, constructivism declares that fact is relevant and depends on someone's perception. It depends on the theory of knowledge that impacts on communication between the investigator and the participants through the research scheme (Carter & Little, 2007).

Constructivism identifies the significance of the meaning of particular human creation as a research paradigm (Charmaz, 2000). According to Searle (1985), it is constructed on the conception of the social erection of the reality that allows the respondents to convey their stories. Moreover, it improves the collaboration of the investigator and the participants. While considering the case of the present study, it has been designed to explore the reality (an investigation of an existing knowledge transfer process for ID theft prevention in the organisation, by investigating the roles of individuals and teams/groups for sharing knowledge of ID theft prevention). The subject: 'existing knowledge transfer process for ID theft prevention,' refers to the truth (the research study problems). The researcher needed to explore the research issue to provide a better explanation of the realism (Lather, 1992).

4.2.4. Interpretivism

Interpretivism is rooted in Hermeneutics and Phenomenology (Blaikie, 1993). Hermeneutics is related to the interpretation of texts and assigning meaning to the text materials (Delanty, 2005; Delanty & Gerard 2005). Phenomenology is associated with how people make sense of the universe around them. The phenomenologists see realism as subjective, which is being socially built by individuals (Bryman, 2015). Hermeneutics is a philosophical practice, which first arose during a period of biblical interpretation in the seventeenth century (Delanty, 2005; Hughes & Sharrock, 1997); it became significant to interpret the scriptures with the growth of Protestant theology. The idea was for the interpreter to reflect with the writer by inflowing his/her mind to understanding the hidden

meanings of texts and the intentions of the author. Such a period of textual elucidation continued to become the basis of the hermeneutic tradition (Delanty, 2005; Hughes & Sharrock, 1997).

Interpretivism's growth was due to the work of authors such as Wilhelm Dilthey (1833-1911) and Max Weber (1864-1920). According to Wilhelm Dilthey, the investigation of the social world must be constructed on understanding (verstehen) the meanings that persons assign to things in their world that cannot normally be explained in substances of the natural world (Hughes & Sharrock, 1997). This needed the understanding of the experiences of persons to comprehend the cultural, social and historical phases of lives of people and the perspective in which certain actions take place (Ritchie, Lewis, Nicholls, & Ormston, 2013). For Wilhelm Dilthey, natural forces cannot determine human actions. Human actions are loaded with cultural meanings and values. The social science investigator enters the social world of other people to understand the meanings which they ascribe to their activities, and then restructures these meanings in the format of descriptions of human action (Ibid). Therefore, he rejected the scientific method as being unsuitable for investigating humans.

Like Wilhelm Dilthey, Max Weber agreed on the significance of understanding (verstehen). However, unlike Wilhelm Dilthey, he was prone to generating causal explanations (Blaikie, 1993). According to him, the social sciences must try to recognise the subjective meaning of peoples' actions to reach the causal explanation for the human action. Social consistencies can be described or understood by knowing the meanings based on human action (Blaikie, 1993). The older hermeneutic belief had stressed that the natural sciences search for causal explanations, whereas the human sciences try to find understanding. Therefore, by merging understanding and explanation, Max Weber marked the conversion from the older hermeneutic practise into interpretative social science; his interest was in social action instead of individual act interpretation (Delanty, 2005).

Interpretivism considers the substantial differences in the research object of natural science and social science. Studying natural phenomena needs the investigator to develop theories and concepts to describe and explain nature. Using theories enables the researcher to make a selection suitable to the problem under study. On the other hand, researching social phenomena needs to understand the social world, which people have built and developed in the course of their routine activities. By such a point of view,

interpretivism rejects the perception that there is an objective realism that can be discovered by investigators. Instead, realism is seen as socially built by human actors. As Blaikie (1993) illustrates, people are continuously interpreting their world via social circumstances and their and others' behaviour. As a result, people develop meanings for their actions and the ideas of making sense of such actions.

Qualitative research has commonly been related to interpretivist practice (Ritchie et al., 2013). Qualitative investigators recognise that various aspects of persons' lives (historical, social and psychological) play a useful part in building an understanding of their world. Subsequently, qualitative investigators employ methods which allow them to get a holistic view of respondents' opinions and activities in the context of their own lives overall (Ritchie et al., 2013). Knowledge sharing processes for ID theft prevention have been investigated, which included how individuals and teams in organisations share knowledge regarding ID theft prevention within and outside their departments. The existing barriers to knowledge sharing for ID theft prevention have also been investigated. Hence, in this study, an interpretivist approach was adopted, which requires delving deeper into the opinions and activities of the respondents to develop new insights.

4.3. The Relevance of Qualitative Research in This Study

Qualitative methods focus mainly on facts, such as what people convey to you, and what they do, via which the researcher will be able to understand what is going on in a particular process or situation. Qualitative research methods illuminate the issues and turn up possible explanations, mainly as an exploration of meaning (as is all research) (Gillham, 2000).

In the qualitative research approach, researchers seek to inspect issues related to the various operations of individuals or groups and teams of people. This method was adopted for collecting stories about individual operations by using the narrative approach. Interviews were conducted with individuals as well as with groups or teams of people to determine how they have personally experienced operations (Creswell, 2014).

This research study aimed to investigate and analyse the knowledge sharing processes within online retail organisations for ID theft prevention. Qualitative research methods were used, as they were more effective at capturing opinions, situations and user responses towards knowledge sharing for ID theft prevention in the organisations

(Bryman, 2013; Myers, 2013). Therefore this study work was based on a qualitative research approach consisting of three case studies.

4.4. Research Strategy Selection

According to Bryman (1984), the selection of a suitable research strategy must be made by the philosophical orientation of the investigator, the research objectives and the research question. The researcher gave consideration to various research strategies, which included ethnography, grounded theory, and case study (Yen-Ku Kuo et al., 2014; Creswell, 2014; Strauss & Corbin, 1990). According to Creswell and Clark (2007), the common strategies of research in the literature of social science are Ethnography, Grounded Theory and Case Study.

4.4.1. Ethnography

Ethnography is a research methodology which uses various data collection methods. It includes participant observation, research interviews, and analysis of documents from the organisation or society, to study the groups, organisations, institutions, and societies; it focuses on capturing and telling the point of view, perceptions, values, inspirations and feelings of the social actors (Silverman, 2013). This methodology is not concentrated on the group, organisation or institution, but it is focused on the behaviours taking place in the organisation and the purposes after the behaviour or recognised activities.

This methodology has an extensive tradition in the field of sociology, and it requires investigators to enter into people's worlds. They investigate for a prolonged period (minimum one year) to understand the phenomena being studied from a societal and traditional perspective of that phenomenon. This means that the role of the researcher will be an integral process of data collection in the field (Smith, 1981). In this methodology, the researchers neither move into the field or natural situation with pre-defined ideas, nor do they interpret the study findings from a theoretical point of view or their viewpoint. Instead, the interpretation of the data takes place through the eyes of the participants in the study (Cavaye, 1996).

Due to the enormous demand for observation in current society, Ethnography has started gaining enhanced acceptance as an interpretive methodology (Silverman, 2013). A frequent criticism of this method is, however, that it is not possible to generalise the

results; these results are established on a small number of cases, sometimes only one case (Ibid). Silverman (2013) claims that it is not durable, as are many disciplines such as psychology, archaeology, biology, and geology, etc. Becker (2008) further claims that these disciplines are unaffected by the use of small case numbers or samples to generate implications and generalisations for a large population.

Ethnography is mainly based on observation, and the role of the researcher would be an integral process of data collection in the field for a prolonged period. Therefore, it was not considered appropriate for this study and was not selected as the research methodology. The main reason for non-selection was that this study did not include observation as a means of data collection due to not having access for observation in the target companies.

4.4.2. Grounded Theory

The researcher gave valuable consideration to Grounded theory as a comprehensive methodology, which refers to a systematic approach for collecting data and its analysis (Strauss & Corbin, 1990). Two American researchers, Glaser and Strauss (1968), developed Grounded theory: by challenging the supremacy of positivism and the quantitative research approach in the field of social sciences, they claimed that the approach of the qualitative method was invalid since it could not be verified. They thought that qualitative methods were not systematic; were descriptive instead of theory generated; and at best played a primary role to the additional 'rigorous' methods of the quantitative method (Denzin & Lincoln, 2000). Due to not finding written guidelines for systematic analysis qualitative data, Glaser and Strauss found it necessary to have a systematic/clear set of procedures to analyse qualitative data (Denzin & Lincoln, 2000; Strauss & Corbin, 1990).

Grounded theory is a qualitative research method, where researchers follow a systematic set of techniques for the development of a theory for a particular phenomenon which is embedded in the data collected (Strauss & Corbin, 1990). It means that generated theory does not come 'off the shelf' but is derived through involving sets of information produced merely on the collected data. If it is undertaken appropriately, the resultant theory fits the dataset accordingly, and should be significant or make sense to those who

have been studied, and should be adaptable and modifiable (Denzin & Lincoln, 2000; Strauss & Corbin, 1990).

In grounded theory, a researcher attempts to develop a theory using numerous steps for collecting the data in a 'zigzag' fashion (Creswell, 2014). The theory develops through the process of research and is derived from the interaction of data collection and analysis (Goulding, 2002). Two main features of the design of grounded theory are the regular comparison of data with emergent classes and the theoretical sampling of participants in the research for maximising the resemblances and variances of information (Creswell & Clark, 2007). Analysis of data starts with data collection, and as a result, the categories occur. Then the researcher proceeds to the field to collect further data or information, which is compared with developing the categories. This continues to the point where there are no new categories to be uncovered. Via the grounded theory, the investigator researches in the real location of the phenomenon being studied, allowing the continuous authentication of themes as the categories occur (Goulding, 2002).

Grounded theory as a method is commonly used when there is no availability of any theories to explain a phenomenon, or there is very little knowledge about a phenomenon, or when the present theories do not adequately discourse the variables of concentration to the researcher (Creswell, 2014; Goulding, 2002).

In several ways, grounded theory could have been suitable for the current research study, although this study used the theory of KM (see Section 2.7 in Chapter 2). The researcher found the theory of KM appropriate for this study as it fulfilled the requirements of the study. Another request of the investigator, to continually return to the location for collection of further data to accomplish saturation, was not possible for this work. Therefore, this study did not use grounded theory for the research methodology. A further reason for not using grounded theory was that this study extended a guiding knowledge sharing framework proposed by Salleh (2010), whereas the grounded theory is useful for developing new theories.

4.4.3. Case Study

Case study research, sometimes known as case research, is a recognised strategy of research in the field of business and information systems. A large number of research publications consider case study research to be one of the best choices of information system research approaches (Carolan et al., 2016; Cavaye, 1996).

Like many other terms, 'case study' has been used in different ways, although it is mostly used for the identification of a particular form of inquiry, one which compares with another two particular social research types, such as 'social survey' and the 'experiment'. Case study methods include the findings of a lower number of naturally arising societal circumstances or cases, and gathering and analysing an enormous amount of exhaustive information about each case. Furthermore, it has been referred to as social research that is comparable under the microscope or in the spotlight (Gomm et al., 2000).

A case study method contains the complete set of procedures required for doing case study research (Hancock & Algozzine, 2015), including case study design, collecting data, analysing the data collection and reporting and presenting the results after the analysis of the data gathered during the case study research (Yin, 2011).

In this research strategy, data collection occurs over a consistent period, as cases are bound by the given time and particular activity; therefore case studies are also known as an investigation of a limited system. A qualitative research approach was adopted in this research. However, a case can use both quantitative and qualitative methods in its conduction (Yin, 2014). According to Hartley (2004), there may be many different ways to conduct case studies. Hartley also focused on the uncertainty of the methods and suggested that others adopt appropriate methods depending on the particular circumstances and the style of their operations.

The case study research approach could be applied to various disciplines which include information systems, business, economics, sociology and many more. Furthermore, case study methods could be applied to understand complex social sensations. It is beneficial in research strategy, where questions such as 'when', 'why' and 'how' are being raised, and when events are less in the control of the investigator, and the investigator focuses on a new spectacle in a real-life context (Yin 2014). In this study, the 'case' is to investigate and analyse the knowledge sharing processes for ID theft prevention in an online retail organisation.

According to Cavaye (1996), it is a multifaceted approach to research and can be applied in different ways and have various research outcomes. It can be used from an interpretive or a positivist viewpoint, with an inductive or deductive technique, or a quantitative or qualitative practice. Case study research is also useful in single or multiple case studies.

Cavaye (1996) outlined various features of case study research through his definition:

- It enables comprehensive understanding of issues in their actual context;
- It allows the investigator to study various aspects of a phenomenon and it also permits the study of a phenomenon not previously determined;
- It is suitable for the development and refinement of the concepts for future research study;
- More than one case study allows the investigator to relate the output to variances in the context.

Furthermore, Benbasat et al. (1987) also recommended three key motives to use in case study research:

- To investigate a phenomenon issue in an actual situation, and to develop the theory from the practice;
- Response from the research queries which may lead to an enhanced understanding of the issue;
- A suitable method in a research area which has previously received limited study.

Yin (2014) argued that there is a misconception that case studies are only suitable for the evocative phase of research and that further research strategies such as experiments and surveys were needed to create explanations and descriptions. Yin also suggested that some well-known case studies had explanatory and descriptive strategies, for example: *"Whyte's (1943/55) Street Corner Society"*. To describe different categories of case studies, Yin (2014) and Stake (1995) used different terms.

According to Yin, case studies could be categorised as *'explanatory'*, *'exploratory'* or *'descriptive'*. Furthermore, Yin also distinguished between the '*single'*, *'holistic case studies'* and '*multiple-case studies'*. Stake (1995) categorised the case studies as '*collective'*, *'instrumental'* and *'intrinsic'*.

An *Explanatory* case study would be used if the researcher was looking to reply to an enquiry that required explaining with the assumed causal connections in real life involvements which are very difficult for investigational strategies or surveys. In

evaluation language, justifications would connect the program application with the program effects (Yin, 2014). *Exploratory* case studies are used to discover the circumstances in which the involvement being evaluated has no vibrancy and a single set of outcomes. *Descriptive* case studies are used to describe an involvement or phenomenon and the real-life situation in which it happened. *Multiple-case* studies are used to explore variations within and between different cases. The main purpose of these case studies is to repeat findings in cases by comparison.

It is important that researchers choose cases very careful so that he/she can foresee identical outcomes across cases, or predict conflicting results grounded on a theory (Ibid). Stake (1995) introduced the term *Intrinsic* case studies and suggested that researchers having a genuine interest in a case should apply this approach to a case study for the intention of a better understanding of the case; it is not assumed primarily as a case to epitomise other cases, or it demonstrates a specific characteristic or problem. The aim is not to understand a certain abstract paradigm or general sensation. Moreover, the purpose of these case studies is not to build a theory.

Instrumental case studies are used to achieve something other than the consideration of a given situation; they enable researchers to have a deep understanding of the issue and the support to refine a theory. In these studies, the case has less attention, as it plays a supportive role and gives help in understanding something else. The case is observed in depth, its situations are inspected, the ordinary activities of the case are detailed, and it is helpful in the research to pursue the exterior concentration. In these case studies, the case may or may not be found to have a characteristic of other cases (Ibid). *Collective* case studies are similar to *multiple* case studies in their nature and description (Yin, 2014).

A recurrent criticism of the approach of case study research is that it is considered to be deficient in rigour. The reason for such criticism of a case study is its interpretive nature and lack of systematic manner; it has been argued it could create a bias in the research study. Another issue raised is that case studies can take a long time to complete and can result in huge and incomprehensible documents (Yin, 2015). However, Yin (2014) claims to overcome these issues through:

- **Construct Validity:** By creating accurate operative procedures for the concepts being investigated. This can be accomplished through the use of several sources of evidence, creating a sequence of proofs, and having the review of the case study report draft from key participants, and to making sure the questions asked were right.

- **Internal Validity:** Internal validity of case studies is useful for causal or explanatory research studies only by building a causal relationship.
- **External Validity:** Through creating the dominion to which the outcomes of research can be comprehensive. This is achievable through the use of theory in *single-case* and *multiple-case* studies using replication logic.
- **Reliability:** Through signifying that the process of collecting data can be repetitive, along with the outcomes. This is achievable through the protocol of the case study.

So far, additional criticism does not generalise the findings of case study research; it is usually considered that case study research findings are not generalisable. The main reason for such criticism is mostly because of the fact of having a relationship between the case study research and the interpretive approach. However, Yin (2014) says that a case study method is also applicable in a positivist enquiry. For the implication of case study in the positivist approach, its purpose is providing analytical generalisations, which can be contrasting to a statistical generalisation of the tradition of the positivist research approach. Yin (2014) considers that case studies, similar to experiments, are generalisable not only to the theoretical propositions but also to the populace or the universe; in this way, the case study, such as the experimentation, does not characterise a 'sample'. The goal of the investigator is to generalise and extend theories, which is called analytical generalisation, but not to contend with frequencies, as in statistical generalisation.

In this research, an *Explanatory* case study approach was adopted, as this study was an investigation of the knowledge sharing processes for ID theft prevention in online retail organisations. This case study approach was used to respond to an enquiry that required the explanation of the assumed causal connections in real life involvements which were too tough for investigational strategies or surveys. In evaluation language, justifications would connect the program application with program effects (Yin, 2014).

Due to the following reasons, the present study selected the case study approach:

- The case study method is useful as it includes multiple techniques of data collection (Bryman, 2013). This study used various data collection techniques for the cross validation of data, including semi-structured interviews, investigation of external and internal documents from the researched companies and the online retail sector.

- The case study method is suitable for this study having the nature to understand a formerly un-researched subject (Yin, 2014). The aim of this study was to investigate existing knowledge sharing processes for ID theft prevention, identify existing barriers in knowledge sharing processes for ID theft prevention and provide an appropriate solution in the online retail sector, which has not been researched so far.
- There is a robust prominence of case studies on research context, which enabled research around the organisation in detail (Bryman, 2013). It was necessary for this research study.

In this research, three different case studies were conducted in three different online retail organisations in the UK. Data were collected using various approaches such as interviews, analysis of internal documents of the organisations (memos, survey reports of the organisation, and much more), investigation of news in print and electronic media, and a web investigation of the organisations.

4.5. Research Design

4.5.1. Overall Strategy of Research Project

This research project was structured into three main phases of completion. Figure 4.1 describes the investigation and development stages of this research study project. The first step was research refinement and finding the gap in the existing research, involving the review of the current area of the research. The researcher used the funnel approach to refine the research of knowledge sharing and ID theft and its prevention (see Figure 2.1). By refining the existing studies in the related area, the researcher found a gap in the existing research. The theory of KM was used to classify the literature and to extend the guiding framework of knowledge sharing proposed by Salleh (2010) in the context of the knowledge sharing for ID theft prevention within an online retail organisation. The existing research gap is provided after reviewing the literature in the area of knowledge sharing, information security, and ID theft prevention.

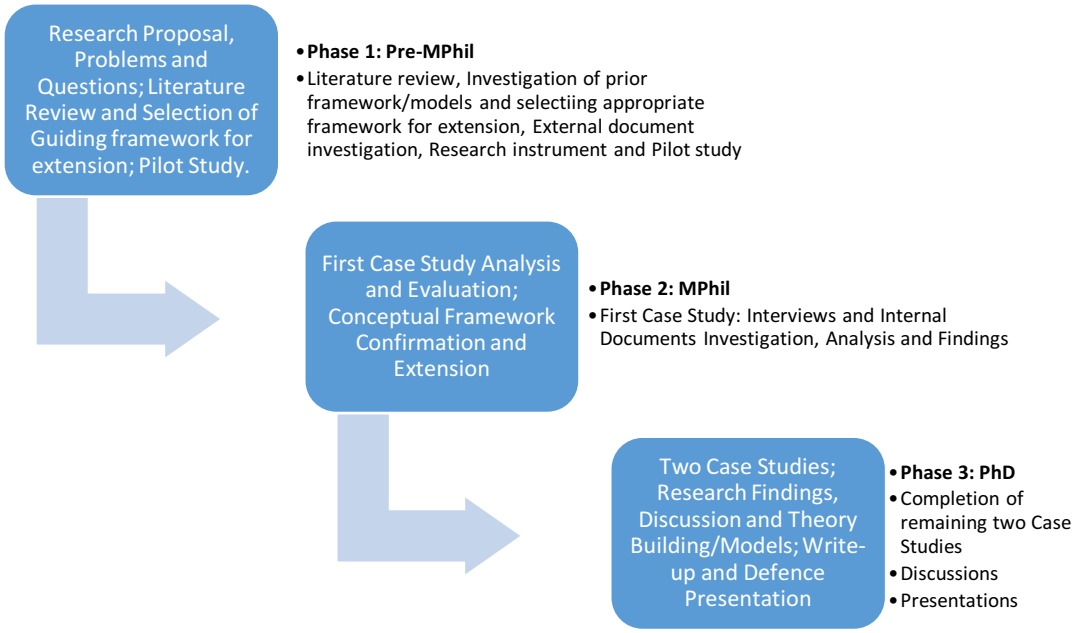

Figure 4.1 Research development stages

The importance, role and use of knowledge sharing for ID theft prevention in online retail organisations were found after reviewing the literature. The researcher found that research work had been previously undertaken in the area of knowledge sharing and ID theft prevention separately. However, the literature review could not find any evidence of research work done in the context of knowledge sharing processes for ID theft prevention in online retail organisations. By finding the research gap and selecting an appropriate guiding framework for an extension, the research instrument was designed for data collection. A pilot study was conducted to test the questions formulated (see Appendix A).

The second stage of the research project included gaining ethical approval for data collection from the concerned body of the University of Central Lancashire. The researcher contacted various companies to gain access to data collection through the supervisory team. One of the target companies (*Company X*) agreed to provide access. A formal agreement for data collection and data security was signed by the researcher and the management of the company. The researcher completed the first case study in *Company X*. On the basis of work done up to that time, the researcher transferred from MPhil stage to PhD stage.

The third stage included the completion of the remaining two case studies including analysis, discussion and write-up, and finally, a PowerPoint presentation was made in defence of the thesis.

4.5.2. Methods of Data Collection

It is noted earlier that case studies comprise extensive data collection (Yin, 2014). In this study, data collection included semi-structured interviews and document analysis (internal and external documents).

- **Interviews**

Case studies were set by eight to twelve interviews. In-depth semi-structured interviews were conducted with the individuals, persons working in teams and groups inside the organisations from top management to lower level staff. Semi-structured interviews were selected for various reasons; they encourage the respondent to talk about issues which are important to discuss and tackle, enable the interviewer to cover some questions about the research (Fielding & Thomas, 2001), and are the best way to save time (Duke, 2002). Furthermore, semi-structured interviews are well known to be easier and more effective than structured interviews or unstructured interviews at the time of interviewing with top management as they enable the researcher to remain in control.

Appendix A includes the research instrument. The interview questions were divided into eight blocks. The first block of research instruments was geared to collect information from the participants. All the other blocks were geared according to the requirements of data collection for this study. The research questions aimed to collect the required data for analysis and around the guiding framework proposed by Salleh (2010) for this research study.

- **Investigation of Documents**

The investigation of documents included internal and external documents from the online retail organisation.

Internal documents were studied and analysed to achieve the aim and objectives of the research. They were examined regarding understanding the existing processes of knowledge sharing for ID theft prevention within the organisation. Various short memos and email conversations, internal policy documents and working procedure documents

were studied to find any evidence of ID theft, reasons for stealing data from individuals and the organisation and the steps taken to overcome those problems, and the existing policies and processes of knowledge sharing for ID theft prevention. The set of internal documents also included secured communication procedures, network security, computer protection procedures, data encryption and many more documents.

The investigation of the external documents included various news reports of the organisations published in print and digital media, which were examined to find any evidence or clues for ID theft and its prevention. Furthermore, the websites of the researched organisations were studied regarding the publications regarding knowledge sharing and ID theft prevention.

4.5.3. Pilot Study

In this research, the interview questions were formed around the factors of the framework. A pilot study was conducted with eight postgraduate students from the University of Central Lancashire. All the steps mentioned by Wengraf (2001) were followed, such as that participant consent was sought from the participants in the pilot, and all the participants were selected by their knowledge and experience in the area of investigation. The pilot study took five weeks to complete. For the interviews, appointments were booked through emails and telephonic contact with participants, and they were informed with plenty of time to allow them to book appointments for interviews. Group study rooms in the library of the University of Central Lancashire were pre-booked as per meetings scheduled with the participants in the pilot.

Face-to-face semi-structured interviews were conducted with the participants. Some additional questions were also asked as per the responses of the interviewees to get clear data for analysis.

In the end, the participants were asked to look for many things, such as repetition and clarity of the questions, and any grammatical mistakes that occurred in the questions. Comments and feedback were considered by revising the interview questions to give more clarity and focus to collect the required data for this research. The terminology of a few questions was changed to enhance the clarity of the questions while asking the interviewees in the interviews. Three questions were removed because of unnecessary and repetitious data received, and four more questions were added to the list to obtain

specific data for analysis. The sequence of the questions was also changed as per the responses of the interviewees during the interviews. Furthermore, the total interview time was checked; the minimum time recorded for the interview was forty-five minutes, and the maximum was seventy-five minutes.

During the pilot, the researcher found that the framework selected for data collection was most specific and it provided all the factors required to collect the data to achieve the aim and objectives of this research. The results from the pilot study included the addition of a few questions to obtain more accurate data and the removal of unrelated and confusing questions from the research instrument. As discussed earlier, the sequence of the interview questions was changed to focus on the required data and maintain control of the interview.

The recording instrument was tested to record the interview with a clear voice, the charging time was tested, and the data storage space of the voice recorder for each interview was also checked. The results from the pilot voice recording device were found to be perfect and ready to conduct real case study interviews for data collection with the online retail organisations, having clarity in voice recording, enough charging capacity, and sufficient data storage space.

4.5.4. Gaining Access to the Companies

According to Yin (2015), a significant element to consider when selecting cases for case study research is having access to data for the prospective situations. For access to multiple cases, it is important for the ability of the case to exclude or answer the research questions. By keeping this in mind, the first thing was to negotiate access to the first intended company through a contact person as a key staff member of the first company.

Through the contact person, an initial formal conversation regarding gaining access was established by email in December 2013. The email conversation included the various documents, for example, an invitation letter about participation in data collection in the research project; a short description of the research project including abstract, aim and objectives of the research; participant consent form; and ethical approval for data collection from the University of Central Lancashire. After the conversation through email, the researcher visited the company. A formal document was signed by the researcher and the company for confidentiality and anonymity of the data, as one of the

critical elements was to ensure and guarantee the anonymity of the company and the respondents.

The confidentiality applied to the name of the company and the participants' responses, and it was assured that none of these should be disclosed either in thesis or published work. Anonymity also included not making any information available outside the organisation. The researcher and the company agreed that the researcher would provide the case study analysis, along with the recommendations, to the company at the end of the study.

After signing the agreement, access was given to the company, and it was necessary to have a key informant for easy entry to the company. It was beneficial to the researcher, as the informant directed the researcher to the participants or other contacts in the company who could be useful in the progress of the research project (Bryman, 2013). According to Reeves (2010), researchers find easier access to data collection through key informants. The researcher found this to be true because the researcher had formal meetings with the key contact person and discussed the study work in detail with the aims of what it was hoped to achieve. The researcher found it easy to arrange meetings with the contact person in the company.

The purpose of that meeting was to convince the contact person that the research project was worth investigation and was in the favour of the company. The report of the findings will be provided to the company. Even though the key contact gave easier access to data collection, Reeves (2010) suggested that key informants can also keep control over the investigation by controlling the participants who do and who do not become part of a study; to overcome such an issue, the researcher ensured that the key contact person was not involved in who was, and who was not, to be interviewed in most of the data collection process. This was done by occasionally requesting to speak to certain individuals within the company that the key contact person may not have suggested, ensuring that the researcher sustained control over the research to the required degree. A total number of 14 interviews were conducted for the first case study in *Company X*.

During the visits to the company, the researcher collected related documents which included memos and internal reports, policy documents and emails. The researcher studied these documents to find any evidence of ID theft, the reasons for stealing the data of individuals and the organisation and the measures taken to overcome those issues, and existing policies and processes of knowledge sharing for ID theft prevention.

For the further two case studies, the researcher drafted an invitation letter which included the aim and objectives of the study and the outcome of the research project. Both the researcher and the director of studies signed the letter. The researcher sent it to 40 online retail companies in the UK in the month of January 2014. Two of the companies responded with interest in taking part in the research. One of the companies (*Company Y*) agreed to provide access in the middle of 2014. The remaining third company (*Company Z*) provided access to data collection at the start of 2015. As with *Company X*, confidentiality was assured, and both the companies expressed the wish to conceal their ID. All three researched companies gave the reason for confidentiality was that they did not want to show their weaknesses, otherwise, customers and other competitors could gain an advantage from it. The researcher accrued the confidentiality and signed an agreement of confidentiality with both *Company Y* and *Company Z*. The same procedure was applied as in *Company X*. The researcher collected 34 semi-structured interviews altogether in this research study, including 14 interviews in *Company X*, 13 interviews in *Company Y,* and 7 interviews in *Company Z.* The data collection also included documents from all these research companies.

4.6. Research Analysis and Write-up

In parallel with the data collection process, the researcher transcribed the interviews. The process of transcribing the interviews enabled the researcher to understand the statements of the respondents in a better way. If there was any conflict in the information provided, the researcher contacted the participant to clarify the information provided. The collected documents were investigated for existing issues of ID theft and its prevention, and the way of sharing the knowledge for ID theft prevention in the researched companies. The analysis included internal and external documents of the businesses and the semi-structured interviews.

At the start, the researcher used NVivo software tool for analysis. Various nodes (codes) were generated to group the responses from the interviews of the participants, which were based on the themes from the framework adopted for an extension, as well as new themes generated in the context of this study (see Section 3.5). These themes included KM Infrastructure, ICT Know-how and Training, Job Rotation, Feedback on Performance Evaluation, Information Sourcing Opportunities, Leadership Support and Knowledge Sharing Culture. During the analysis process, the researcher put all the data from the

interview transcripts into the NVivo nodes. After putting the data into NVivo nodes, the researcher printed all the grouped responses (in nodes) along with the references (interview transcripts and documents) and analysed them manually by reading all the responses in each node and sub-node. The researcher used both the NVivo software tool and a manual approach for coding and analysis of the data.

As with other PhD studies, this study was expected to address the posed research questions. However, the current study did not make any generalisations in the online retail sector. Based on the findings of this study, it successfully showed how the researched companies presently manage this problem. Following that, it made recommendations. Furthermore, the enhanced concepts will illustrate the developments in the online retail organisations regarding enhanced knowledge sharing processes for ID theft prevention. The literature review mentions (Chapter 2) the online retail organisations' need to increase their knowledge sharing processes for ID theft prevention. Therefore, an extension of a framework of knowledge sharing for ID theft prevention will be useful to the online retail industry organisations. The findings of this research study are valid as these have emerged from the online retail organisations. All the researched companies are major players in the online retail industry; two of the three researched companies are in the category of being in the top 10 online retail organisations in the UK.

4.7. Chapter Summary

This chapter included the methodology of the research study. To answer the research questions posed in the introduction chapter of the thesis (Chapter 1), the researcher paid attention to various approaches of the research philosophy and emergent methodologies for its adoption, describing the adopted philosophical approach and the strategy for the research of this study, including the research design; only those having relevance were reported. The perception for philosophical adoption emphasised the beliefs of the researcher for the nature of reality and potential ways of obtaining knowledge.

The literature classifies the research methods into two categories: quantitative research methods and qualitative research methods. Quantitative research methods are usually associated with the 'positivist' philosophy and are held with quantification, replicability, objectivity and causality. By the use of a massive quantity of data, quantitative research shows itself to use statistical methods which are applied in analysing the results.

Quantitative research methods usually include a survey as an instrument of inquiry. However, experiments and secondary analysis of the data can also be used. Those methods focus on facts instead of judgements.

The philosophical grounds of qualitative methods are commonly associated with phenomenology and hermeneutics, where prominence is applied to inspecting the social world from the view of the actors. Hence, qualitative research investigators try to cultivate a critical understanding of the issues under study through data collection in the actual place where the players are involved in the problem under investigation. The present research study selected qualitative research methods for the inquiry of knowledge sharing processes for ID theft prevention in online retail organisations.

Every research method has strengths and weaknesses, though the selection of a suitable strategy for research depends on the type of investigation questions posed and the degree of control the researcher has on the research themes. The current research study used an interpretive approach. The strategy was based on the use of case studies.

The method of data collection included semi-structured interviews and investigation and analysis of documents from the researched companies (internal documents) and outside the companies (external documents). For the analysis, an NVivo software tool was used along with a manual coding and analysis process.

CHAPTER 5 DESCRIPTION OF EMPIRICAL WORK

5.1. Introduction

This chapter includes the description of the empirical work undertaken for this research study, describing the findings of three case studies completed in online retail organisations. The UK online retail organisations were selected for two main reasons. The first is UK online retailing, worth £60.04 billion in the year 2016, with a growth of 14.9% from 2015 (Newark Beacon Innovation Centre, 2016), around 5% of GDP (Gross Domestic Product), that consists of 10% of all employment. UK online retailing includes Consumer Healthcare, Beauty and Personal Care, Media Products, Consumer Electronics and other online retailing. As mentioned in the report of the Centre for Retail Research (CRR) in 2016, UK online sales were £60.04 billion in the European market, which includes seven European countries (Germany, France, Spain, Italy, the Netherlands, Sweden and Poland). The UK is the top country in the list, having the largest amount of sales in the year (CRR, 2016). Therefore, the UK's retail sector is considered to be an important indicator for the participation of other Organisations for Economic Co-operation and Development (OECD) countries.

The second is UK E-retailing that had been the initiator for implementing the process of electronic trading. The history of online retailing in the UK is much stronger and has its emphasis on internet-based trading. The tendency is that digitised retail processes and business transactions require the provision of personal sensitive information through debit and credit cards. UK retailers have an opportunity, provided by the internet, which can help, to match this tendency, but does not exclude the issues originating from ID theft. In socio-economic terms, the retail industry tracks the livelihood of customers in the UK, and impacts on the ability of customers who buy online to respond to the issue of ID theft. The online retail sector is considered one of the main sectors where consumers are more prone to the theft of ID, with a small amount of investment in the prevention and knowledge sharing for ID theft prevention.

Due to this, the online retail sector in the UK offers a unique venue to understand the nature of ID theft issues and prevention of ID theft and investigation of knowledge sharing processes for ID theft prevention in businesses. In this study, the researcher consulted numerous online retail companies, which were considered to be an appropriate

selection to conduct this case study design (Yin, 2015). In total, three online retail companies (*Company X*, *Company Y* and *Company Z* for anonymity) were selected. All the companies were chosen for semi-structured interviews and analysis of internal and external documents. The companies were selected on three factors. Firstly, collecting data for the case studies from several firms enabled the researcher to apply a "*case-replication*" methodology for testing the implications of these research findings in different cases (Yin, 2015). Secondly, the culture of the business, size (large to medium to small) and ethics of the companies were taken into consideration, as their involvement in the online retailing field and e-commerce are known to be the strategies which are commonly adopted by the online retail industry throughout the world. Thirdly, it was important that online retail companies were willing to facilitate and participate in taking the research study, and confirmed that they would provide the data needed; they were also interested in the feedback from this investigation.

Furthermore, to add to the factors above, Norman K. Denzin and Yvonna S. Lincoln (2005) laid great emphasis on selecting research cases by opportunities to gain access and to learn from them. Marshall and Rossman (2014) also recommended the requirement of a fundamental mix of procedures, personnel, contacts and structures of curiosity to be present in the selection of cases in a research study. The chosen organisations hold the distinguished and well-structured culture of a business and practices which offered ample opportunities for gaining access to these companies, along with contacts to top management (Wilson, 2014). The selected companies were involved in a series of 21st century advanced methods of online retailing business activities and were well-known online retail organisations in the UK.

The companies were selected by three criteria which included the location of the branches within the UK because the locations chosen best matched the research strategy of the researcher in respect of the base university. This enabled the researcher to have quick access to the participants of this study easily, on time and for less expense (Hakim, 2000). It also gave access to supplementary data; as it is a conventional investigation, the more data there is, the better it is. The researcher had time to conduct interviews and analyse the collated data simultaneously, including the investigation of documents collected from the researched companies.

5.1.1. Investigation of Documents

The retail companies chosen for the archival analysis included the selected researched companies which enable consumers to directly purchase goods or services from sellers on the internet by browsing their websites, including retail organisations which use online shopping and processing of services in the form of business-to-business (B2B). The case analyses did not include the banking sector, due to the direct connection to online retail business operations with digital banking. The online retail firms co-operate with banking sectors for handling the consumers' identities and approval of the payments when completing the online purchasing process. To obtain answers to the research questions of the current nature of ID theft related issues and existing knowledge sharing processes for ID theft prevention in online retail organisations, the analysis was based on archival resources of the UK.

The analysis contains ID theft related issues and knowledge sharing for ID theft prevention empirical research reports from various sources; for example, digital libraries, website portals, magazines, newspapers and archival newsletters, special reports, annual reports and other relevant electronic resources of organisations. The archival means were fortified by the interpreted business reports by the UK Financial Service Authority and British Retail Consortium (FSABRC), which increases previous research works by analysing a diverse period on interrelated ID frauds and the knowledge sharing processes for ID theft prevention. The contents of reports were critically analysed, along with the reporters'/authors' perspectives, and the contexts of ID theft incidents. In order to have access to data from these sources, a search was conducted for reports and articles that contained, but were not bound to, the following terms in the abstract, keywords and title: *identity theft, identity frauds, identity issues, identity theft detection, identification, mitigation, propagation, prevention, business information security, identity, identity theft prevention, knowledge sharing, knowledge sharing about identity theft prevention, and information systems security management.*

To understand the existing knowledge sharing processes for ID theft prevention in online retail organisations, this research required internal documents from the researched companies. The researched companies agreed to provide these at the request of the researcher, who ensured the confidentiality and anonymity of the companies regarding the documents collected. During the visits to the companies, the researcher collected the related documents which included memos and internal reports, policy documents and

emails. The internal documents were studied and analysed to achieve the aim and objectives of the research and were examined regarding understanding the existing processes of knowledge sharing for ID theft prevention within the organisation. Various memos, internal reports and emails were studied to find any evidence of ID theft, reasons for stealing data from individuals and the organisation, and the steps taken to overcome these problems.

5.1.2. Semi-Structured Interviews

For the semi-structured interviews, three online retail organisations, *Company X, Company Y* and *Company Z* (renamed for anonymity) were selected. They were selected because they are online retail companies and take part in online selling and purchasing of products and services.

These organisations comprise various sizes (large, medium and small) and were selected to provide a complete understanding of the research study problem of this research project: The investigation of the knowledge sharing process for ID theft prevention in the online retail organisation. It mainly focused on studying and investigating how individuals and teams, groups or departments share knowledge for ID theft prevention with each other.

Semi-structured interviews were selected for various reasons: they support the respondent to discuss issues which were important to tackle; enabled the interviewer to cover some questions of the research (Fielding & Thomas, 2001), and were premium to save time (Duke, 2002). They are also known to be easier and more effective than strongly structured interviews and unstructured interviews at the time of interviewing with top management, as they enabled the researcher to remain in control.

5.2. Knowledge Sharing Processes for ID Theft Prevention in *Company X*

The first case study of this research project was completed in *Company X*. The selected company is the leading multi-brand retailer with approximately £2 billion annual sales, having millions of active customers receiving millions of products every year. More than three-quarters of the sales at this company take place online, one-third of those being from mobile devices. About one million customers visit the company website every day.

At the start of collecting the data, the investigator made a formal agreement with the management of the company, according to the ethical approval gained from the parent university, to make sure that the research was conducted as per the University Code of Conduct. The research ethics was significant and a 'must do' in the present study, and it provided informed consent to the participants and also valued their right of privacy. The investigator made initial contact with the senior management of the case company. *Company X* provided access by signing an agreement of confidentiality for the first case study.

In total, fourteen interviews were conducted in various departments in *Company X*. All the participants were selected according to their working experience and speciality of knowledge of information security, ID fraud prevention and its knowledge sharing. One of those fourteen interviews was conducted by telephone, and the remaining interviews were face-to-face. The researcher visited various branches of the company in different cities to conduct the interviews.

The procedure of having the alternative of either a telephonic or face-to-face semi-structured interview allowed the investigator to gain the prime support of the contributors (David, 2004). Having multi-method data collection, it provided the chance to investigate the internal documents of the company as, during the visits for the data collection process, the contact person and the interview participants provided various documents for analysis. Documents were collected to investigate the existing methods of ID theft prevention, the policies of awareness for the staff in protecting their organisational knowledge, and the current procedures for ID theft identification and prevention. These documents included various policy papers, email conversations and memo reports.

Table 5.1 List of interview participants in *Company X*

Participant Code	Position of Participant	Participant Department	Participant Job Responsibility	Participant Experience	Interview Duration
CX-R01	Fraud Prevention Manager	Group Security	Performance management.	9 years	50 Mints
CX-R02		Fraud Prevention	To action referrals, speaking to actual customers who have been the victims of ID theft and solving their issues for them.	8 year	70 Mints
CX-R03	Fraud Prevention Advisor	Fraud Prevention	Looking at online applications for credit. Dealing with victims of ID theft, attending to calls from victims and explaining to them what to do and helping them.	10 years	45 mints
CX-R04	Head of Intelligent and Technical Lead	Group Security	Internal consultancy.	10 years	51 mints
CX-R05	Regional Loss Prevention Manager	Group Security	Fraud and theft investigation and prevention.	24 years	60 mints
CX-R06	Information Security Manager	Group Security	Threat detection, threat management and vulnerability scanning.	1 year	45 mints
CX-R07	Technical Security and Training Development Manager	Group Security	Group security head of technical services and training.	14 years	67 mints
CX-R08	Information Security Specialist	Group security	Information security specialist, making sure that customer data is safe; encryption of sensitive information.	10 years	58 mints
CX-R09	Group Security Director	Group Security	Head of different departments. Consulting with the managers of various departments, especially group security, information security and fraud prevention departments.	10 years	60 mints
CX-R10	Loss Prevention Manager	Fraud Prevention	Investigation of fraud and theft within the business.	17 years	65 mints
CX-R11	Security Intelligence Analyst	Intelligence Unit	Supporting the regional loss prevention managers in their role and providing the information they require.	9 years	49 mints
CX-R12	Support Analyst	Group Security	Analysis of data and putting packages together and sending them out to the regional director.	6 years	55 mints
CX-R13	Intelligence and Technical Lead	Group Security	Intelligence and technical lead.	9 years	62 mints
CX-R14	Security Intelligence Support Analyst	Physical Security	Investigation of ID theft regarding hijacked accounts, fraudulent set up of accounts and investigation of the web during the process of the fraud being committed.	6 years	52 mints

An interview is helpful for the interviewer to understand and notice the behaviour and feelings of the interviewee (Bryman & Bell, 2015). The researcher used this approach as a procedure by conversing with 14 selected participants to produce research data for the first case study (Denzin & Lincoln, 2011); the job titles and working responsibilities are shown in Table 5.1. The participants had working experience ranging from one year to twenty-four years in the company. Some of the participants were already acquainted with the significance of data security and the need for ID theft prevention as they had been involved in various operations and activities for ID theft identification and prevention within the company. To decrease the bias and to enhance the validity, numerous interviews were conducted (Yin, 2015), which enabled the investigator to ensure uniformity and constancy in the data by including the facts, opinions, and expected knowledge. Each interview continued for 45 to 75 minutes depending on the interviewee and his/her responses.

5.2.1. KM Infrastructure

Technology is a major factor in implementing a prosperous KM program and approach and is an effective source for creating, storing and sharing information. Information and communication technologies infrastructure refers to effective KM based on persons sharing their knowledge through technological facilities that users throughout the organisation have access to. In an organisation, updated information and the communication technologies infrastructure help the employees to generate, store and share knowledge between individuals, teams and departments (Syed-Ikhsan & Rowland, 2004). Investigation of the existing KM infrastructure was prioritised to determine limitations and provide proper recommendations for enhancing the knowledge sharing for ID theft prevention.

During the interviews, questions were asked to investigate the existing infrastructure including the software, hardware, networks and protocols developed for information security in the organisation and the skills required for knowledge sharing. Further questions were asked about the availability of resources and to investigate the usefulness of the KM resources and any requirements for more resources (see Appendix A).

While asking about knowledge sharing tools being used for sharing knowledge for ID theft prevention, participants reported that various tools were being used for ID theft prevention, such as CIFAS, AQAFAX and KBA (CX-R03). The research found that for

sharing knowledge, the company has an e-learning system which provides information on training available to staff members; employees also upload their activities on the e-learning system. Respondent (CX-R01) said:

> *"We have many systems that we use. I think for knowledge sharing the strongest that we use are the e-learning packages; if anything new comes out such as a new process, or new system, it is always done through e-learning."*

Furthermore, policy documents are being uploaded onto the intranet of the company, and sometimes workers acquire their knowledge by using personal contacts. According to (CX-R08):

> *"So it is a combination of both personal contact and also the intranet, written policies and written information, which is available to all."*

To acquire the information technology skills required for knowledge sharing for ID theft prevention, it was found that basic skills are provided to staff members in the company. For example, how to use and create Excel spreadsheets and pivot tables (CX-R11; CX-R12). A few of the staff members are trained to analyse the data by their experience regarding ID fraud and encountering those frauds (CX-R08). The employees have a basic level of skills, but they are satisfied with the availability and usage of the existing resources and having the skills developed from their experience to work in the company and use the existing systems.

5.2.2. ICT Know-how and Training

ICT refers to information communicated by using telecommunication systems. ICT infrastructure plays a vital role in knowledge sharing among the individuals within and outside the organisation. It is essential to understand the ICT skills required to assess the ability of staff who use those skills to solve the complicated problems of information management, knowledge sharing and presentations (Cobo, 2013). These include learning and technical expertise such as developing ideas, sharing information and fact finding (Cobo, 2013; Dede, 2010). Employees require particular practical skills and 'know-how' to perform required tasks efficiently. These can be learned and developed through independent learning/detecting and emulating the skills of others, which are the approaches of tacit knowledge sharing environment (Letmathe et al., 2012).

An advanced learning environment enables the workers to enhance their expertise to deal with complicated problems. Learning opportunities enhance progress by removing previous mistakes and weaknesses (Harteis et al., 2008). Various organisations provide different training opportunities for their employees to keep them up-to-date and to enhance the innovative techniques to improve their performance.

The researcher asked various questions on training regarding knowledge sharing in the organisation and to investigate the effectiveness of the training provided to the workers to enhance their skills of the knowledge sharing for ID theft prevention and to determine the opportunities for increasing it (see Appendix A).

From the responses to the question *"How do you get training to enhance your skills for knowledge sharing for ID theft prevention in your organisation?",* interviewees responded that such training is provided for fraud prevention and to understand existing systems in the organisation. If a new system comes into their department, then the company provides training to staff to enable understanding and operating those systems and provide knowledge about its functionalities (CX-R01; CX-R03; CX-R12). If new employees join the company, they get induction training for 12 months to understand the existing systems and their job role (CX-R07).

Participant (CX-R11) responded that they had basic training to use and create spreadsheets in Excel and Access at the start, but acquired knowledge from their own experience. They did not receive further training. He/she responded that:

> *"We have had Excel training, spreadsheets, Access database training, things that we would need to produce our reports to the regional loss prevention managers. As for the fraud side of it, we have not had much training ourselves. It is self-taught."*

CX-R11 responded that if a new system or tool comes in, training is given to understand that system and the availability of training is being discussed in daily 'huddles' (internal informal meetings).

A few participants responded that training to identify and prevent ID fraud is provided to the workers in the fraud prevention department only (CX-R11; CX-R13); the remainder responded that training is not being given to them at all (CX-R11; CX-R12). When asked for reasons why training was not being provided, the interviewees responded that they

did not need training, as they are not working at the front end and do not face customers directly. Participant (11) stated:

> "*We are not dealing with the customers; we are dealing with the aftermath of what happens. I do not think we are dealing with everything that's passed down to us; we do not need that training as such at the moment."*

Another respondent (CX-R14) stated that these days, fraudsters are smart and fast; ID fraudsters have adopted new techniques and methods to commit fraud and training does not help them to stop the fraud. This research found that, at the moment, the company provides other learning opportunities for the workers, such as one-to-one meetings, the arrangement of seminars, and updates in meeting 'huddles' regarding ID related fraud identification and prevention (CX-R02). When asked about the advantages and usefulness of these learning opportunities, the participants responded that training could be advantageous (CX-R01; CX-R08; CX-R10; CX-R13).

When asked about the training provided for the knowledge sharing for ID theft prevention, all the responses were "*No*". Currently, the company does not arrange any training for sharing the knowledge for ID theft prevention. Participants even stated:

> *"…we are not doing anything like that; we do not need training for sharing the knowledge of ID theft prevention."*

This investigation found that training and other learning opportunities can play an important in enhancing the knowledge of employees for ID theft prevention. Participants required a learning environment to share their knowledge for ID theft prevention among staff members. Presently, the company focuses on the prevention of personal information theft at the customer level, and they are not focusing on the development of an enhanced knowledge sharing processes for ID theft prevention within the company. Therefore, it is recommended that they develop an environment of the knowledge sharing for ID theft prevention among individuals and groups/teams within the company.

5.2.3. Job Rotation

Knowledge shared among individuals is linked with establishing communication among workers inside an organisation. The most significant issue of knowledge sharing is the trust within the organisation such as, how willing are people to share what they know? Answering this question leads us to activities based on trust building, team creation, job

rotation and so forth (Sveiby, 2001). Job rotation plays a vital role in enhancing the knowledge of individual employees and teams within and outside any department in an organisation (Aga et al., 2016; Huang & Pan, 2014; Ortega, 2001).

While investigating the job rotation process, the researcher found that jobs are not being rotated except via promotion from one position to another. According to interviewee (CX-R13):

"There isn't any job rotation."

Moreover, interviewee (CX-R10) responded:

"We do not do any rotation really with anybody else."

As discussed earlier, job rotation plays a vital role in increasing the knowledge of individuals and teams in the organisation, but in the company, employees are learning from their experiences. Participant (CX-R01) replied that jobs are not being rotated from department to department to enhance the knowledge of ID theft prevention. One of the interviewees responded that their job could be moved from one seat to another seat if someone was not coming to work or someone was sick, so to fulfil that requirement of work, employees are moved to other seats (CX-R01). If someone requires some information, he/she puts the question forward and obtains the knowledge for that question. Respondent (CX-R03) said:

"If you want to learn something you can always put the question forward."

While asking the reason for not rotating jobs in the company, the respondents said that they are all doing the same job; the company does not need to rotate the jobs.

Currently, the company does not rotate jobs to increase staff knowledge for prevention of ID theft and to share their knowledge for ID theft prevention with others in the organisation. It is strongly recommended that the company develop a job rotation process so that individuals and team members may enhance their knowledge and learn from the experiences of workers moved from other areas who have expertise via their work in ID theft prevention. The staff whose job has also been rotated increased their knowledge by working in a new environment.

5.2.4. Feedback on Performance Evaluation

Feedback is vital for the evaluation and monitoring of activities of employees. However, current developments in electronic technology are advancing the nature of monitoring the performance of employees (Alder & Ambrose, 2005).

Feedback can be given for various purposes, which include bringing the resultant outcomes of the activities or the processes into focus; providing information when workers move away from primary goals; helping them to fix new goals or adjusting the current goals, and guiding perform their activities. It also promotes critical reflection and brings about new approaches (Gabelica et al., 2012).

To investigate the performance of employees, various questions were asked about feedback. Participant (CX-R01) said:

> *"That is the bulk of the managers' job; we have performance management."*

The researcher found that managers arrange monthly one-to-one meetings with the advisors to ask how things are going and how staff are performing their activities. Feedback is given to employees by the work done and the level of success. The company also evaluates the performance of employees twice a year (CX-R10).

Asking about the tools being used for assessing the performance of employees, the respondents said that they have only one tool for evaluating the performance of employees, which is an e-learning system providing knowledge of evaluation modules (CX-R08; CX-R10; CX-R13; CX-R14). Respondent (CX-R14) said that:

> *"It is an e-learning module. Each worker has to score a hundred percent. If they do not, they have to re-sit it until they get a hundred percent in both ID theft and ID fraud. However, yeah, that is the only measurement in place."*

For evaluating the performance of knowledge sharing with others, managers and advisors responded that the company is not evaluating the performance of employees on knowledge sharing processes for ID theft prevention. Participant (CX-R10)'s response was:

> *"As for ID theft prevention and knowledge sharing, we are not evaluated on that."*

For the impact of feedback, participants said that it is vital to assess the performance of work activities. By assessing the performance of employees, their managers do have the knowledge that an employee is doing well and he/she has the knowledge of their working

activities. They also know that staff are working as per the requirements and policies of the company. Furthermore, if they notice that someone requires training or cannot work, then that employee should be trained, or someone should help him/her in the working role. The managers provide the feedback to staff in a one-to-one meeting or through email detailing how they are doing their work and what they need to increase and whether they need to go through a re-training process.

The company needs to determine at what level employees learn about knowledge sharing regarding ID theft prevention and provide feedback to the workers.

5.2.5. Information Sourcing Opportunities

For enquiring about information sourcing opportunities, all the respondents stated that information regarding ID theft issues and their solutions are being shared through email, policy documents and the internal network messaging system. For investigating the preferred method of sharing knowledge, the respondents stated that they prefer to use emails to receive information (CX-R07; CX-R08).

The participants used emails as a knowledge sharing resource as emails provided most of the updated information regarding ID theft issues and their solutions. They were easier to use and to attach documents to and to send to the recipients. Furthermore, emails have quick access everywhere. Participant (CX-R11) responded:

> *"Email is fast, and you can put whatever you like in it and attach documents, and that is the main source we have always used."*

According to the participant (CX-R14), employees are being emailed to inform them about the availability of training. A participant said:

> *"Email is the best way, and I receive emails for the availability of training."*

Regarding the satisfaction from the available sources in the company, the researcher found all the participants were satisfied with the availability of knowledge sharing resources. However, for sources of sharing knowledge with staff from other departments, the participants responded that they send and receive the required information through emails only.

Currently, the company uses the emailing system for disseminating information and some policy documents providing useful knowledge to the employees regarding the working

environment and activities which use the secure IT infrastructure. They also have an internal messaging system called 'Yammer' in which employees post updates of working activities (CX-R01; CX-R03; CX-R10).

5.2.6. Leadership Support

Leadership support is one of the most important elements in enhancing the working environment of the organisation and encouraging staff towards achieving the required goals. During the investigation, the researcher found that management shares information regarding ID theft issues through emails and monthly meetings. Participant (CX-R01) said:

> *"We have managers' meetings every single month; we have a buzz of managers' emails."*

Managers also arrange face-to-face meetings with workers (CX-R02; CX-R10). An internal network messaging system is also being used to share the knowledge to identify and counter issues; they call it the 'blackboard'. Additionally, management arranges seminars to update the workers' knowledge of ID theft and its prevention. Some participants from the fraud management and information security departments stated that they needed a more technical workforce to prevent ID theft in the company. While managers and staff members were happy with the support of the leadership (CX-R03), the participants, however, required quicker feedback. Interviewee (CX-R02) responded:

> *"... quick feedback accreditations; all that is needed for you to be able to do your job in there successfully."*

One of the managers required more staff as they cover the whole of the country (R10), stating:

> *"You can always do with more individuals to help because we cover the whole country. So more resources would be more workforce."*

The leadership of the company is very supportive of the workers, and the staff are happy with the facilities provided to them. Sometimes line managers walk down to the desks of the advisors and other employees to help them and to describe the activities performed to identify and counter ID fraud.

This investigation found the leadership of the company very supportive and helpful, and the employees were happy with them. When talking about ID theft prevention knowledge sharing, again there is the need for an enhanced environment of knowledge sharing for ID theft prevention. The support of management is required for the development of such an environment so that individual staff members and teams can share their knowledge for ID theft prevention across the departments in the company.

5.2.7. Knowledge Sharing Culture

Knowledge sharing refers to the sharing of awareness among individuals, different teams and departments inside the organisation and various organisations. Organisational culture relates to the shared values, beliefs and performances of persons within an organisation (McDermott & O'Dell, 2001). Knowledge sharing culture is the main element considered for knowledge sharing among the individuals and teams in any organisation and is the most important factor that needs to be understood in advance before employing any new strategies in an organisation (Syed-Ikhsan & Rowland, 2004).

A knowledge sharing culture is considered to be a significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM. According to Stoddart (2001), knowledge sharing can only work if the culture of the organisation supports it, and if the changes required are developed according to the culture of the organisation.

In this regard, the researcher investigated the knowledge sharing culture in the company. Interviewees stated that they trusted the other workers to share the knowledge ID theft prevention within their department, but they did not trust the people outside their department in the company. Presently, knowledge is being shared only within departments of the company (CX-R01; CX-R12). Employees are not confident enough to share knowledge with the staff of other departments to prevent ID theft due to a lack of trust (CX-R07). Therefore, individual staff members and teams are only getting the advantage of the expertise within their department. The company needs to develop a system to educate the staff from different departments and increase the awareness of ID theft and its prevention. They need to increase the level of trust within the organisation.

From the investigation of internal documents of *Company X*, the researcher found that the company has a clear policy on the secure usage of the existing facilities of the company.

Those facilities include computers, databases and communication networks and ways of communication. Users are restricted from spreading information outside the organisation. From the investigation of email conversations and policies for use of emails, the researcher found that the company's e-communication and tele-communications services are made available to users for business purposes. A certain amount of limited and accountable personal use is allowed by staff but under rigorous guidelines. The company rules apply to anyone retrieving and using the email facilities made available by the business based at any site.

These rules apply to all permanent, temporary, contracted and part-time employees. While using the email system of the company, individuals should make sure that all conversations with others reflect the ethics and professional standards of the company. The Information Security Department is responsible for ensuring that the usage of emails is appropriately monitored and controlled in compliance with these security policies. From the emails and memo conversations of the managers, the researcher found that if any issue of ID theft arose, the directors of the company advised the information security department to sort it out.

At the moment the company has secure network connections. From the investigation documents, the researcher found that the company has the policy to define the connection standards between the company's IT network and any external host, ensuring that data transportations to and from exterior systems are accomplished securely. Following that policy reduces the exposure to the risk of damage which can be caused by the unauthorised entrance or the use of the company's electronic assets, which could constitute damage to critical internal systems, loss of sensitive data, intellectual property and damage to public image.

The company has secure use of mobile devices in the business. From the investigation of internal documents related to the usage of secure mobile computing, it was found that the company does not allow devices containing customer data outside business premises. If this is not possible and there is a good reason for using these devices outside the company site, then it must be permitted in writing by the authorised personnel at that site; it would be the responsibility of the individual using that device to seek that requirement.

Table 5.2 Summary table for strengths, weaknesses and recommendations of *Company X*

Factor	Strengths	Weaknesses	Recommendations
KM Infrastructure	- Uses tools for ID theft prevention such as CIFAS, AQAFAS and KBA. - Has an e-learning system for updating the employees regarding available training.	- Available training is being uploaded, but that e-learning system does not provide knowledge for ID theft prevention. - The infrastructure is not being used for knowledge sharing for ID theft prevention.	- A knowledge sharing system is required so that employees can share knowledge with each other and learn from others' experiences to prevent ID theft.
ICT Know-how and Training	- Training system for the new employees. - Provides policy documents for working activities. - Arranges seminars to enhance the knowledge of the workers.	- Fundamental training to the employees, such as how to create spreadsheets in Excel and Access when joining the company. - Only staff from the fraud department are trained.	- Need to enable the employees of departments to have training in ID theft prevention. - Develop a knowledge sharing system for ID theft prevention. - Develop the education of the workers in the process of knowledge sharing.
Job Rotation	- The company does not employ job rotation.	- No job rotation. Individuals from non-technical departments and teams are not benefiting from others' experience.	- Need job rotation to enhance the knowledge sharing process for ID prevention.
Feedback on Performance Evaluation	- The performance of the employees is being evaluated as per working activities, and feedback is given on results.	- Not assessing the performance of knowledge sharing of employees for ID theft prevention.	- Need to assess how much employees know for knowledge sharing regarding ID prevention and provide feedback.
Information Sourcing Opportunities	- The company has a policy of ID theft prevention. - Uses an internal network messaging system to broadcast information within the company and emails to update employees on ID theft issues.	- Individuals are not sharing their expertise and methods regarding ID theft prevention.	- More resources could be provided to the staff for the knowledge sharing for ID theft prevention. - E-learning system could be enhanced as a source of knowledge sharing for ID theft prevention and increase the skill levels.
Leadership Support	- Leadership is very supportive of the workers and staffs are happy with the facilities provided.	- More workforce is needed to prevent ID theft.	- Leadership could facilitate the staff to educate them in how to share the knowledge for ID theft prevention. - Technical education and training are needed for a better environment.
Knowledge Sharing Culture	- Different teams get the advantage of knowledge sharing. Staffs are trusted. - Employees are happy with existing IS.	- Personnel from other departments do not benefit from the knowledge. Less trust in staff from other departments.	- Need to increase the trust level. - Need to educate the workers from other departments to share knowledge.

From the investigation of the internal documents, this research found that the company is robust in securing its IT facilities which include computers, mobile devices, communication networks and other media. However, the researcher did not find any evidence of focusing on enhancing the knowledge of individuals and teams/groups for ID theft prevention within the company.

During the investigation, it was found that currently, the company provides induction training to newcomers on the existing systems and working activities at a basic level, such as spreadsheets and fraud databases (see Table 5.2). An e-learning system is used to upload the information for the training and educational seminars which are arranged. However, the company does not have a training system for the knowledge sharing for ID theft prevention.

An advanced learning environment enables the workforce to deal with the complex problems faced. The company still needs to allow the staff of all departments to receive training regarding ID theft prevention practice and prevention. Table 5.2 summarises strengths and weaknesses in *Company X* for the knowledge sharing for ID theft prevention and recommendations from the investigation of this research.

The emailing system is used for information sharing amongst the staff; sometimes an internal networking system called 'Yammer' is used to update the employees regarding ID theft issues. At the moment, the company uses CIFAS and AQAFAX as tools for knowledge sharing for ID theft prevention. The company needs to enhance the knowledge sharing culture for ID theft prevention; currently, individuals are sharing their knowledge with each other within a department, and they trust those who are working with them within that department; therefore, staffs of other departments are not getting the advantage the knowledge sharing for ID theft prevention.

As a result, also recommended is the development of a system for the knowledge sharing for ID theft prevention and the education of the workers in the process of knowledge sharing. From the investigation of the internal documents, the researcher found that *Company X* is competent at securing the IT facilities including computers, mobile devices, communication networks and the other media. However, the researcher did not find any evidence of focusing on enhancing the knowledge of individuals and teams/groups for ID theft prevention within the company.

5.2.8. Existing Barriers to Knowledge Sharing for ID Theft Prevention in *Company X*

During the investigation of the knowledge sharing processes for ID theft prevention, this study found the following obstacles:

- **Staff Unwillingness**

Staff willingness plays a key role in the process of knowledge sharing. The literature describes that measures taken for knowledge sharing depend highly on the willingness of the employees working in the organisation (Hislop, 2002). According to Scott Holste and Fields (2010) and Hislop (2002), the attitude of workers to share their knowledge can be motivated by their awareness of their responsive connectivity with their working organisation. These perceptions impact on the willingness of staff members to their commitment to the organisation. Employees who have satisfaction in their jobs and commitment to their companies are willing to share their knowledge and believe in the advantages of the organisation as being for their benefit (see Table 2.11). Individual staff unwillingness can be a barrier to the knowledge sharing processes for ID theft prevention in an organisation.

During the investigation, the researcher found that individual staff members are willing to share the knowledge of ID theft issues and its prevention with others within their department.

Participant CX-R02 responded that:

> *"I am happy to share information with my friends working with me, but not ready to share with others."*

However, employees are not willing to share any knowledge with others outside their department in the company. Participant CX-R10 said:

> *"Why would I share knowledge with others, if they cannot help me anyway?"*

While enquiring about the reasons for not being willing to share knowledge with others outside the department, this research study found that there is no environment of knowledge sharing for ID theft prevention outside of the department; there are no rewards or incentives of sharing knowledge with others (CX-R04; CX-R11). Therefore, individuals are not willing to share their knowledge with others. Another reason for staff unwillingness is that the rules and regulations bind them, so they cannot share the

knowledge with anybody who does not work with them unless anybody needs help to solve an issue (CX-R14). Therefore, staff unwillingness is a barrier in the knowledge sharing for ID theft prevention.

- **Lack of Staff Awareness**

Individual staff awareness is essential for the success of the knowledge sharing processes in an organisation (Ismail & Yusof, 2010). It is considered to be a tool for enhancing co-operation and sharing knowledge in the collective process (Daneshgar, 2001). Employee awareness of the knowledge sharing processes encourages the individuals to share their knowledge efficiently and provides the chance for creative thinking to handle complicated issues and understand the mistakes of others (Safa et al., 2016). According to Van den Hooff et al. (2003), any organisation that is in a phase of unawareness cannot comprehend the influence of knowledge sharing processes against its competitors. Therefore staff, including management, must be aware of the importance of sharing knowledge for an effective knowledge sharing culture in an organisation (see Table 2.12).

This research study found that there is a lack of awareness in the individuals and teams regarding sharing the knowledge for ID theft prevention. A participant responded:

> *"I do not know about the knowledge sharing for ID theft prevention."*

They are not aware of the advantages of knowledge sharing which can enhance their knowledge to tackle issues (CX-R06). One of the participants stated:

> *"Why should we share it, I do not need it. I learn from what I do."* (CX-R10).

The researcher found that there is a lack of awareness of the processes of knowledge sharing. Participant CX-R02 said:

> *"I do not know about the process of knowledge sharing, I do what I need to do, but if they provide training for this, I will be happy to attend."*

In *Company X,* the lack of individual staff awareness is a barrier to the knowledge sharing for ID theft prevention. The company needs to provide a learning environment to educate the staff for the knowledge sharing processes of ID theft prevention.

- **Insufficient Learning Opportunities**

A learning environment provides opportunities leading to increased capabilities and skills by routine work (Mohammad Hossein & Nadalipour, 2016). Learning opportunities are known to be key factors in the efficient employment of a knowledge sharing programme

for employees (Cong & Pandya, 2003). There can be various learning opportunities to enhance the knowledge of staff members working in any organisation, and training is one of those learning opportunities useful for increasing the knowledge of employees in a company. Training is helpful to enhance technical skills in computer usage and knowledge sharing (Hortovanyi & Ferincz, 2015). Many organisations arrange different training opportunities for employees to keep them up-to-date and increase knowledge (De Grip & Sauermann, 2013; Dymock & McCarthy, 2006). According to Luu (2013) and Peter A.C. Smith (2012), the lack of a learning environment in any organisation is a barrier to enhancing the knowledge of individuals and teams.

While investigating existing learning opportunities, the researcher found that the company provides learning opportunities to staff members working in the business. They provide training to staff members newly joining the company (CX-R03; CX-R10), however, this training is provided regarding the existing infrastructure of the company, for example, how to interact with the computerised systems in the company, what the effective procedures are, and how to deal with customer data.

The company has some refresher courses to update the staff with new changes in the infrastructure if a new system is implemented (CX-R06). However, this training is not provided to enhance a knowledge sharing environment for ID theft prevention, and only staff from the fraud prevention and information security department receive training for ID theft prevention. Furthermore, currently the company provides other learning opportunities to the workers, for example, one-to-one meetings, seminars, and updates in meeting huddles regarding ID related fraud identification and prevention (CX-R02).

The participants require further training to enhance their knowledge of ID theft issues and its prevention. However, the lack of learning opportunities is the barrier in the processes of knowledge sharing for ID theft prevention in *Company X*.

- **Distrust of Other Staff Members**

According to Pan and Scarbrough (1998), an atmosphere of trust is essential for knowledge sharing; it is known to be one of the key elements in the processes of knowledge sharing (Bălău & Utz, 2016; Hashim & Tan, 2015). Staff will work more efficiently if they trust other staff members working with them (Safa et al., 2016; Roth & Broad, 2008; Hsu et al., 2007; Bos et al., 2002; Ridings et al., 2002; Jones & George, 1998). Various empirical studies have supported the importance of trust in sharing

knowledge in an organisation (Rutten et al., 2016; Safa et al., 2016; Hsu et al., 2007). Distrust can deter the practice of knowledge sharing in an organisation (Willem & Buelens, 2009).

The present study found that staff members trust other workers within their departments. On the other hand, they do not trust employees working outside their department, and they are reluctant to share the knowledge for ID theft prevention with people with whom they do not work. Interviewee (CX-R05) responded:

"I do not trust others outside of my working unit."

Participant (CX-R10) said:

I cannot share knowledge with people who are not here in this department."

Therefore, individual staff members and teams get the advantage of knowledge sharing and learning from others within their department at work. The lack of trust is a barrier to the processes of knowledge sharing for ID theft prevention in *Company X*.

- **Fear of Information Leakage**

Information leakage is a big issue for any organisation. Therefore, data protection is a big challenge for companies to manage from unauthorised access within and outside the company, so information leakage has become a main concern of online retail companies (Marabelli & Newell, 2012; Trkman & Desouza, 2012; Desouza, 2006; Desouza & Vanapalli, 2005). The growth in issues of disclosure of sensitive information has had considerable coverage in the media and by researchers (Abecassis-Moedas & Rodrigues Pereira, 2016). Research studies emphasised various significant aspects of data leakage, which included insiders working in the organisations (see Table 2.15). Companies are very much restricted in the protection of their resources and data.

From the investigation of the documents of *Company X*, the researcher found that the business has strong rules and regulations for the protection of the ICT infrastructure and information. However, there is a lack of awareness of the processes of sharing knowledge about the issues of ID theft and its prevention. Due to these strict rules and policies, staff members have a fear of leaking information into the wrong hands. Staff members are not ready to share the knowledge of other staff members to enhance their knowledge for the protection of ID theft (CX-R10; CX-R14). Participant CX-R01 said:

"I am afraid that others can leak the information I give them. So, I do not discuss with others for identity theft."

Respondent (CX-R04) stated:

"We do not trust people we do not work with. They can leak data. So why should I share any knowledge with them?"

In the company, staff have a fear of data leakage, and therefore they do not share their knowledge of ID theft prevention with staff members of other departments. The researcher found that fear of information leakage is a barrier to knowledge sharing for ID theft prevention in the company.

- **Insufficient Information Sourcing Opportunities and Inefficient ICT Infrastructure**

The ICT infrastructure includes the intranet, communication networks, emails, data warehousing, and the decision support system. It is necessary for knowledge sharing in the organisation (Stankosky, 2005). Stronger ICT facilities are essential for the availability of knowledge and enhanced knowledge sharing process (Khan et al., 2016).

On the other hand, information sourcing opportunities help people to share knowledge with each other; it is essential for any organisation to have effective information sourcing opportunities (see Table 2.16). Weaker ICT infrastructures and inefficient information sourcing opportunities can fail the knowledge sharing process in any organisation (Syed-Ikhsan & Rowland, 2004), as ICT infrastructure helps the employees to generate, store and share knowledge between individuals, teams and departments.

The researcher found that *Company X* has a strong ICT infrastructure; staff use tools for ID theft prevention such as CIFAS, AQAFAS and KBA and they have an e-learning system for updating the employees regarding available training (CX-R03; CX-R12). However, the e-learning system does not provide knowledge for ID theft prevention, and the existing ICT infrastructure is not being used for knowledge sharing for ID theft prevention (CX-R10; CX-R13; CX-R14).

The present study found the company has various information sourcing opportunities, for example, policy documents provide information about how to deal with ID theft issues (CX-R07). Staff use the internal network messaging system to broadcast information within the company, and emails are also used to update employees on ID theft issues.

However, these opportunities are not being used for sharing the knowledge for ID theft prevention, and individual staff members are not sharing their expertise and methods regarding ID theft prevention.

From the investigation, the researcher found that the company has an excellent ICT infrastructure and good information sourcing opportunities for securing both customer and organisational information. However, the existing infrastructure and sourcing opportunities are not being used for enhancing the knowledge of individuals and teams for ID theft issues and its prevention; therefore, it is a barrier to knowledge sharing for ID theft prevention in *Company X.*

- **Lack of Leadership Support in Knowledge Sharing**

Leadership plays a major role in managing the knowledge sharing processes in any organisation (Muethel & Hoegl, 2016); therefore, it is accountable for practising strategic planning for the best use of means and promoting a learning culture and knowledge sharing (Boerner et al*.,* (2007). The top management should provide support to encourage the importance of knowledge sharing and be responsible for the support to signify knowledge sharing approaches (Mittal & Rajib, 2015). Table 2.17 in the literature review chapter describes the importance of the leadership in the processes of knowledge sharing.

This research study found that the leadership of *Company X* is very supportive. Participant (CX-R01) said:

"Managers are good and always help me. They provide all facilities I need here".

In various ways the management shares knowledge with staff members; they use emails to update employees working in the company (C-R10). A participant responded:

"... my managers send me email for the updates."

Line managers and other levels of managers have meetings to update staff (CX-R08). Sometimes, management calls relevant persons working in the company and discuss the issues and working progress. Line managers even walk to the desks of staff and have discussions with them (CX-R02). The researcher found that staff are happy with the management of the company. However, there is a lack of leadership support for enhancing the knowledge of individual staff members and teams to share the knowledge for ID theft prevention, and currently, they are not focusing on strengthening the knowledge of staff regarding ID theft prevention awareness. This research study found the lack of leadership

support to be a barrier in the process of knowledge sharing. The support of the management is required for the development of such an environment so that the individual staff members and the team can share the knowledge for ID theft prevention across the departments in the company.

- **Weak Knowledge Sharing Culture**

Organisational culture refers to the shared values, beliefs and performances of persons within an organisation (McDermott & O'Dell, 2001); therefore, it is one of the main elements considered in the organisation for knowledge sharing among the individuals as well as the teams, and this needs to be understood in advance before employing any new strategies in an organisation (Syed-Ikhsan & Rowland, 2004). A knowledge sharing culture is considered to be the most significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM (see Table 2.18). Therefore, a weak knowledge sharing culture can be a barrier in the process of knowledge sharing in any organisation.

At the moment individual staff members share their knowledge with other colleagues within their department (CX-R09; CX-R11). Respondent (CX-R02) said:

> *"We do not share knowledge with others, but we do share knowledge here in our department".*

On the other hand, there is no culture of sharing the knowledge for ID theft prevention in different departments in *Company X*; there is no culture of sharing knowledge for ID theft prevention. The weak knowledge sharing culture is a barrier in *Company X*.

- **No Job Rotation**

Job rotation plays a vital role in enhancing the knowledge of individuals and teams within and outside any department in an organisation (Aga et al., 2016; Huang & Pan, 2014; Kane et al., 2005; Ortega, 2001). Table 2.19 shows that it increases the knowledge of individual staff members, and enables them to discover their strengths and weaknesses (Santos et al., 2016). According to Eriksson and Ortega (2006), employee learning, employer learning and employee motivation are the main advantages of job rotation in any organisation; furthermore, it enables individual staff to learn from various departments, decreases employee exhaustion caused by tedious or boring job tasks and increases both the individual's confidence and the satisfaction in the job.

This research investigation found that there is no job rotation in *Company X;* all participants responded with "*No Job rotation"*. The lack of job rotation results in no enhancement in the knowledge of individuals and teams in the organisation (CX-R06). No job rotation leaves the individuals to learn from their own experience and is a barrier to knowledge sharing for ID theft prevention in the organisation. It is an obstacle to knowledge sharing for ID theft prevention in *Company X*.

Table 5.3 Barriers to knowledge sharing for ID theft prevention in *Company X*

S.No	Barrier in KS for ID theft prevention	Empirical Findings in *Company X* (Barrier in KS for ID theft prevention)
1	Staff unwillingness	Yes
2	Lack of individual staff awareness	Yes
3	Insufficient learning opportunities	Yes
4	Distrust of other staff members	Yes
5	Fear of information leakage	Yes
6	Insufficient information sourcing opportunities and inefficient ICT infrastructure	Yes
7	Lack of leadership support	Yes
8	Weak knowledge sharing culture	Yes
9	No job rotation	Yes

Table 5.3 shows the existing barriers in knowledge sharing for ID theft prevention in *Company X.* This study found staff unwillingness, lack of individual staff awareness, insufficient learning opportunities, distrust of other staff members, fear of information leakage, insufficient information sourcing opportunities and inefficient ICT infrastructure, lack of leadership support, weak knowledge sharing culture and no job rotation are barriers in the process of knowledge sharing in *Company X*.

The case study findings from *Company X* show that individual staff members are not willing to share knowledge with others. Another reason for staff unwillingness is that the rules and regulations bind them. There is a lack of awareness in the individuals and teams to share their knowledge for ID theft prevention. The company needs to provide a learning environment to educate their staff in the knowledge sharing processes for ID theft prevention. The current learning opportunities are insufficient and are not being used for sharing the knowledge for ID theft prevention. While talking about trust in other staff members in the company, staff trust at their departmental level and share their knowledge of working activities within their departments in the company. There is a need for knowledge sharing between individual staff members and teams in non-technical

departments to enhance their knowledge of ID theft issues and its protection. The existing knowledge sharing culture does not support enhancing the knowledge of individual staff members working in non-technical departments of the company. There is a fear of information leakage in the company. Due to that fear, staffs are not willing to share their knowledge with others, and it results in not sharing the knowledge for ID theft prevention. The company has good information sourcing opportunities and ICT infrastructure.

However, these opportunities and the ICT infrastructure are not being used for the awareness of staff members to enhance their knowledge of ID theft prevention. The leadership of the company is helpful to the staff working in the company, but they do not support the processes of knowledge sharing. The literature clarifies that job rotation is a fundamental element for enhancing the knowledge of individuals and teams in any organisation. However, *Company X* does not utilise the policy of job rotation in the company. Staff are learning from their own experience.

5.3. Knowledge Sharing Processes for ID Theft Prevention in *Company Y*

The researcher conducted a second case study in *Company Y.* The company is a corporate company having multiple child companies selling online train tickets, processing online payments and maintaining online travel schedules; over 3,000 employees joined the company in the year 2015. *Company Y* manages the information of 1.3 billion passengers with payment processing and travel information. The online database of the company is considered to be one of the biggest databases in the Europe, storing passengers' travel schedules, payment processes and so on. The company is responsible for managing its child companies, selling online tickets and providing customer information.

The same procedure applied for gaining access as in *Company X,* although it was difficult to get access into *Company Y* due to the busy schedule of staff in the company. After waiting for a few months the researcher finally obtained access to data collection, and during multiple visits, the second case study of this research project was completed, which included thirteen interviews with various levels of staff members in multiple departments of *Company Y*. During the data collection at *Company Y,* the researcher conducted twelve face-to-face interviews and one telephonic interview.

Table 5.4 List of interview participants in *Company Y*

Participant Code	Position of Participant	Participant Department	Participant Job Responsibility	Participant Experience	Interview Duration
CY-R01	Microsoft Technical Lead	Group Business Services	Look after the Microsoft estate including cloud infrastructure. Make sure that anything entered conforms to the right standards.	15 years	55 mints
CY-R02	Project Manager	Asset Management	Support IBM infrastructure. IBM officer application service infrastructure and IBM WebSphere Messaging infrastructure.	1 year	60 mints
CY-R03	Senior Application Support Analyst	Information Management Department	Responsible for managing data migration, data security, hardware and software setup.	5 years	63 mints
CY-R04	Project Manager	IT Department	Accountable for managing a technical team.	2 years	50 mints
CY-R05	Project Manager	Project and Programme Services	A trainer, e-Learning, research and development. Helping people's needs with the right frameworks and proper regulations.	16 years	70 mints
CY-R06	Procurement Assistant	Supply Chain	Manage delivery of work stream. Working on desktop transformation programme.	2 months	46 mints
CY-R07	Project Manager	PMPS	Managing the communication in the company. Sending out communication emails to individuals and teams.	1 year	49 mints
CY-R08	Communications Writer	Desktop Transformation Program	Supporting the regional loss prevention managers in their role and providing the information they require.	1 year	48 mints
CY-R09	Business Development Manager	Supply Chain	Commercialisation of excess capacity from the supply chain including selling of goods and services to third parties.	2 years	50 mints
CY-R10	Business Support Specialist	Supply chain	Commercialisation of excess capacity from the supply chain including selling of goods and services to third parties.	1 year	51 mints
CY-R11	Project Manager	Corporate Functions	To deliver business change, new technology, to time, to cost and to quality.	5 years	66 mints
CY-R12	Procurement Manager	Maintenance and Development	Maintaining the ICT-infrastructure of the company.	3 years	50 mints
CY-R13	Head of Information Security	Information Security	Responsible for securing the information. Looking after information security issues.	2 years	67 mints

Table 5.4 shows the list of participants along with their working responsibilities and experiences. Furthermore, the company provided the required documents which included their existing policies and rules to protect the assets of the company and any evidence of knowledge sharing for ID theft prevention in the company. Additionally, the collected documents included information regarding securing computers, network security, database security, data encryption and so on.

5.3.1. KM Infrastructure

At the moment the company uses different tools for knowledge sharing among the staff members, including Yammer, a centralised system (they call it Connect), Share Point 2007, emails, an e-learning system and LYNC (CY-R12). Policy documents are uploaded onto the website of the organisation and can be accessed by individuals using their user ID and password (CY-R03).

While inquiring about the satisfaction with the availability of resources for knowledge sharing for ID theft prevention, the researcher found participants were happy with the availability of resources for knowledge sharing. However, these resources are not being used to share their knowledge of ID theft prevention in the company.

Participant (CY-R10) said:

> *"I am happy with the system we got, but I am not sure we use them for ID theft…"*

Respondent (CY-R12) replied with:

> *"I am pretty satisfied because the way the IT systems work here, there are quite a lot of checks and balances in place which will avoid such a problem."*

Participant (CY-R07) responded:

> *"We have got many resources that we share information with. I think probably out there; we are one of the best companies in it."*

Interviewee (CY-R08) stated:

> *"I am not sure what resource is used to prevent our identities being stolen."*

All participants seemed happy with the usage of the existing resources.

Participant (CY-R06) replied:

"Well, it is hard to think of it regarding ID theft so far because that does not come with a lot of what we do. But, yeah as in the same resources that you use day-to-day are the same ones that are always safety critical. So when you share resources like SharePoint, it will show who's modified it and when. Moreover, you can look and see who has access to it so, who can see the documents. "

Participants in *Company Y* require IT skills regarding awareness about securing personal and organisational information. A couple of participants required knowledge of informatics and secure usage of existing systems and website of the company.

Participant (CY-R11) responded:

"IT knowledge just the ability to sign on to an application, and also being sensitive about data and confidentiality of data. So it is a skill to control access to your password."

Participant (CY-R12) required training for the prevention of ID theft. He/she answered:

"From an ID theft perspective, I think the regular training or IT skills are just generic for normal day-to-day use. I do not believe there is a specific training for that here that we receive. However, of course, cyber fraud and prevention of ID theft, prevention of any such access are always recommended."

The researcher found the participant happy with the existing KM infrastructure in the company. All the resources they need for their job role are available to them, and they are satisfied with the usage of the existing resources. However, knowledge regarding the prevention of ID theft in the company is not being shared, and currently, the company is not focusing on enhancing the knowledge of staff to understand ID theft issues and their prevention. Employees demand awareness of ID theft issues and how to protect against them.

5.3.2. ICT Know-how and Training

For the investigation of *"How is training provided to improve the skills of employees in the company?",* the interviewees responded that all employees pass through training (CY-R10; CY-R07) which includes inductions, refresher courses and scheduled training. The company arranges training for newcomers: induction. Induction is provided company-wide and at the departmental level. During the company-wide induction, the employees

are taught about the infrastructure of the organisation, which includes information about the buildings and the culture of the institution. In the departmental induction, staff are introduced to the working environment of their department, the equipment, the software, and the way in which new staff members are required to work.

Interviewee (CY-R3) responded:

> *"When you join the company is usually you have an induction to the building and the culture of the institution as a whole, and you have building introduction where you get your security passes and access and things like that. Moreover, there are also departmental inductions. Moreover, then within the job role you got, then you got your specific training for."*

While enquiring for the job role training, the research found that all employees are being trained according to their job roles. If someone new joins a team, then other members of the team train the newcomer. Participant (CY-R10) said:

> *"If someone comes into my team then the person who was working in the team would be training the new person now."*

The majority of the participants said they had fundamental training to use computers and perform their job roles, for example how to use computers and the existing software tools for day-to-day activities, including use of Microsoft Office, the emailing procedure, how the supply chain is laid out, how to make a purchase and the products on sale.

At the moment the company has different methods to train its employees. They have a monthly meeting, and various issues are highlighted in the meetings such as what the issues are and how to solve them. A training team provides a demonstration of what the problem is and how to solve it. The company has a training platform, which is called *"Skill Soft";* using that platform, the management of the company updates the staff about existing electronic systems if a new system is being introduced in the company.

While asking about information security related training, the respondent (CY-R07) said:

> *"There's a cyber security section in it where we are keeping sort of information security training".*

At the moment the company is not providing any training for ID theft prevention. When the researcher enquired about the availability of training for ID theft prevention,

participant (CY-R10) said, *"There is no mention of ID theft",* and participant (CY-R01) responded, *"There is no training for ID theft prevention in the company".*

This research found that the company is not providing any training for ID theft prevention (CY-R06; CY-11; CY-R12). While investigating the reason for not providing training for ID theft prevention, participant CY-R08 responded, *"I think it would be useful. I am not sure why they do not arrange"*. A couple of interviewees answered that they do not need such types of training because they are not directly dealing with the customers (CY-R02; CY-R09).

Currently, the company has provided additional learning opportunities to the staff members, which include group meetings at the team level, open days, and various seminars for awareness to the staff (CY-R02). Employees are highly satisfied with the availability and usage of learning opportunities in the company and with the existing learning opportunities to help them in their day-to-day jobs, communication with each other and the use of the current ICT environment.

The company does not provide any training for sharing the knowledge for ID theft prevention. All the participants answered *"No"* to the question, *"Does your business provide any training for ID theft prevention knowledge sharing among the staff?"* The company does not have any policies which focus on ID theft prevention and to enhance the knowledge of individuals or teams within the company. While asking for the requirement of other learning opportunities to improve the knowledge for ID theft prevention, most of the participants responded that if the company provided any training courses, they would be happy to attend.

As discussed earlier, a healthy learning environment plays a vital role in increasing the knowledge of employees for ID theft prevention. Staffs require an educational (learning) culture for knowledge sharing for ID theft prevention in the company; currently, the company emphases protecting customer information from fraudsters and ID thieves. Therefore, it is recommended that they build a culture of the knowledge sharing for ID theft prevention in the company and educate individuals as well as teams and groups.

5.3.3. Job Rotation

During the investigation, this research found *Company Y* very strong in job rotation. While asking about job rotation, all the participants responded with *"Yes"* to the question *"Does your company do job rotation?"* When a new member of staff joins the company,

his/her job is rotated around different departments to understand the environment of the organisation and job role in the company. Participant (CY-R01) responded that:

> *"...our graduate training programme, when the graduate starts right after university to join us, we have got very structured training programmes for them. So they take six months' role in different departments of their choice."*

There is another process of job rotation in the company, which is called "secondment". In this process, staff member joins a new department for a specified period and can return to the previous department if he/she does not fit in or cannot settle for the new job role for any other reason. Participant (CY-R10) replied:

> *"So once your secondment is finished, let's say you worked there for six months, you can go back to your job. You will not lose that job. So you can learn something new ... if you do not find a permanent position in your new team, you can go back."*

To move into a new department, the staff need to pass through the selection process of the new job. If he/she passes the screening process, they can join the new department or team.

Individuals are getting the advantage of job rotation in the form of enhanced knowledge about other departments and other job roles. They learn about new systems which were not used in previous departments and get knowledge from the experience of others in the host department. They learn by doing something new in the new job role and experience new things. Participant (CY-R11) said:

> *"...because they do something different, it expands their experience. It means that we do not have a single point of failure because somebody else can do his or her job too."*

Respondent (CY-R12) said:

> *"It is just by gaining knowledge of different areas."*

Regarding advantages for teams and departments from job rotation, the researcher found that the company is getting the full advantage of spreading the knowledge of groups and teams across the departments. Staff move from one department to another department or from one team to another team and share their expertise with others in a team or group. When the secondment period finishes and the individuals return to their home department,

the people in that department get the advantage of their experience and the new knowledge gained during that time.

Participant (CY-R10) said:

> *"Yeah because let's say if someone comes into my team then the person who was working on the team would be training the new person now."*

For the advantage to the teams, the respondent (CY-R11) replied:

> *"It means that they do not have a single point of failure. They got other people they can rely on. You do not get one person who has all the pressure."*

Whereas, for the usefulness of job rotation for increasing the knowledge of employees for prevention of ID theft in the company, this research found that job rotation does not play any role in enhancing the knowledge of individuals in the organisation for ID theft prevention. Departments are not getting the advantage of knowledge sharing for ID theft prevention from the people of other departments. The company is not rotating jobs to increase the knowledge of persons for ID theft identification and its prevention.

From the findings, it is clear that the company has a strong job rotation process, which can play a major role in increasing the knowledge of individuals, teams and groups to prevent ID theft.

5.3.4. Feedback on Performance Evaluation

The company is quite good at evaluating the performance of the employees; all staff members pass through the assessment process.

Participant (CY-R12) said:

> *"All employees, when we do the performance appraisals, they are looked at regarding what innovation or knowledge development they have done."*

At the departmental level, managers meet one-to-one with the staff every month to check the performance of the staff and provide feedback. Feedback is provided by working activities, tasks completed and the behaviour of the staff with others in their department or team. Meetings are held in separate rooms, and relevant managers provide feedback to the staff. The company evaluates the performance of employees twice a year. Every employee needs to fill in a pro forma they call an 'appraisal'.

Participant (CY-R04) stated:

> *"That is a quite strong area for this company ... there are target setting and performance setting in place for employees. There is six months and twelve months sort of reviews of the job, and so there is quite a strong focus in that area, and I would say the company is very, very mature in this field."*

At the end of the year, every staff member needs to fill in an appraisal for the performance of the year.

Respondent (CY-R11) replied:

> *"Employees have to write it annually; they call it end-of-year or half-year performance review."*

The company has an e-learning tool that is referred to as an e-learning portal which is used to evaluate the knowledge level of the employees. Different courses and online training are uploaded on the e-learning portal. Individuals go through these courses and test their knowledge levels.

Participant (CY-R06) responded:

> *"So, getting on courses, doing e-learning, making sure you know the procedure, understanding the procurement process, understanding values, and things like that."*

For evaluating the employees' performance for knowledge sharing for ID theft prevention with others, the researcher found that the company is not evaluating performance in that context.

Participant (CY-R01) said:

> *"ID theft is not one of those criteria. It is all about your job, how you have done your job."*

Feedback on performance evaluation has a positive impact on the working activities of the staff, and the employees are happy to be evaluated on their performance. Participant (CY-R08) said:

> *"This is the main way of evaluating performance, just our manager watching us over a period and seeing how we are improving. Moreover, then we also have*

feedback sessions with managers and people above or below us so that all of the information can be visible to everyone."

Line managers and departmental managers provide the feedback by evaluation on the performance of staff. The research found that the company is solid in the performance evaluation of their employees. Apart from that, the company is not focusing on sharing the knowledge of employees for ID theft prevention. There is no system to evaluate the performance of knowledge sharing for ID theft prevention in the organisation.

Therefore, the company needs to implement an evaluation system for knowledge sharing activities and knowledge awareness of the employees in the context of ID theft prevention.

5.3.5. Information Sourcing Opportunities

This research found that the company has various sources of information sharing, for example, they use emails to share information (CY-R11; CY-R10). Staff receive numerous emails for their working activities and much more. The company has a website for internal use and employees can access it through their identification and passwords. They use SharePoint 2007 as the centralised system for updating the employees (CY-R01). The company has an internal messaging system called 'Yammer' for use within the company.

Company Y has implemented various sourcing opportunities to update their employees, such as the e-learning portal available on the website, and using PowerPoint presentations to update their staff (CY-R06; CY-R11). Employees also access policy documents on the website. Furthermore, there is a library in the building which is used as a source for enhancing knowledge.

Staff do not use any messaging on their phones. Participant (CY-R1) responded:

"We do not use IM for that type of thing."

While investigating the preferred information-sharing source, almost all participants considered email to be their preference for getting information. Interviewee (CY-R12) said:

"I always prefer emails."

Staff use email as a knowledge sharing resource because it provides them with updated information regarding any issues and day-to-day job activities. Email is available to access everywhere, and it is easy to send documents. It allows quick access by staff members anytime.

On the other hand, a few participants responded with different choices. Participant (CY-R05) preferred the intranet for communication purposes. He/she said:

> *"I like using Link. I prefer it because I know that the person is there, that they are available and I can contact them, and I can get a response."*

Participant (CY-R07) responded:

> *"For me, it would be a sort of a policy document or some briefing. ... I can read it in my own time and hopefully absorb some of the information. Alternatively, if it is a quite interactive briefing the information will go in because I am focusing on it."*

This research found that the company has various information sourcing opportunities provided to the staff, for example, the staff have access to the e-learning system which is called the 'e-portal' in the company. They use a messaging service called 'Yammer'. The employees access SharePoint, the emailing system, arrange seminars and street shows. The management update the staff using PowerPoint presentations and a huge library exists in the company building which contains an enormous amount of literature for employees to enhance their knowledge.

Staff have various information sources to update their knowledge, but the company is not focusing on the awareness of ID theft issues and its prevention. Existing systems can be used for sharing knowledge for ID theft prevention. Individuals, as well as teams, can use these opportunities to enhance their knowledge for ID theft identification and prevention.

It is recommended that they build a knowledge-sharing environment to facilitate the individuals and groups/teams within and out of the departments for ID theft prevention in the company.

5.3.6. Leadership Support

Supportive leadership plays a vital role in the working environment in the organisation and motivation of individuals and teams to achieve the goals required. The management of *Company Y* is very supportive and share information with staff in different ways; they regularly send group emails for general issues and task completion. Participant (CY-R04) said:

> *"There is a cascade of information being done via email, and so there are regular email briefings that come out as well as obviously the emails, cascade emails as well."*

Now the company has implemented an internal messaging system called 'Yammer', which is a semi-social network within the company and each employee has access to it. The management of the organisation use that tool for uploading information about new events and issues and also for group discussions where staff can ask for help and guidance regarding their routine work and other activities.

Middle-level management and line managers provide instructions via individual emails and group meetings (CY-10; CY-R08; CY-R04). Line managers meet staff one-to-one and listen to them if they have any issues or problems that need to be solved. Departmental managers arrange regular group meetings for the staff and share knowledge of the working processes, workload and achievement of tasks (CY-R01; CY-R04; CY-R07). The management of the company arranges conferences and seminars for employee awareness.

Regarding expected support from the leadership of the company for sharing the knowledge for ID theft prevention, the researcher found that staffs require guidance and education for ID theft issues, how to prevent it, and how to protect personal and organisational knowledge from unauthorised persons. The participants also required knowledge sharing sources to be available to them and the enhancing of the business systems for ID theft prevention. Participant (CY-R12) said:

> *"Support regarding training, education and guidance. Moreover, just making resources available, making business systems robust enough to protect from ID theft and promote knowledge sharing from that perspective."*

Participant (CY-R03) responded:

> *"I expect my ID to be secure in which of our systems they are keeping it in. I should have access to it when I need to know that what information they keep about me."*

The participants required the policy about ID theft issues and ID protection.

Interviewee (CY-R04) replied:

> *"If there is a policy in the organisation about knowledge sharing or ID theft, then certainly everyone will be expected to comply with it. I think there will be top support, high-level support certainly."*

Although the leadership of the organisation is very supportive of the staff, and the workers are satisfied with the facilities provided to them, while talking about sharing knowledge for ID theft prevention, protection from ID theft issues and providing awareness of ID theft prevention it was noted that this is not the focus of the leadership of the company. The majority of the staff require education and awareness about ID theft issues and securing their own and organisational knowledge. The employees demand the support from the management to implement a knowledge sharing environment and create a culture of the knowledge sharing for ID theft prevention.

5.3.7. Knowledge Sharing Culture

According to McDermott and O'Dell (2001), organisational culture includes the shared values, attitudes and performances of individuals in an organisation. Knowledge sharing culture is the key component considered to share the knowledge amongst the individuals and teams in the organisation. It needs to be understood in advance before retaining new approaches within the organisation (Syed-Ikhsan & Rowland, 2004). It is also considered to be an important aspect since it pedals the impacts of other elements of knowledge sharing processes in the organisation, for example, existing technology and management techniques on the accomplishments of KM. Stoddart (2001) says that knowledge sharing works if the organisation's culture supports it.

This study found a strong culture of knowledge sharing in *Company Y*. The staff trust each other and share knowledge within and outside their department in the company (CY-R01; CY-R06; CY-R10).

While investigating the confidence of others for sharing the knowledge for ID theft prevention, the researcher found that knowledge regarding ID theft prevention is not the focus of staff. Individuals trust each other to share knowledge about regular jobs and day-to-day activities in the company.

Participant (CY-R10) responded:

> *"I expect people to tell me, people, I work with. If I am doing something wrong because I work quite closely, it is open plan. I am sitting next to somebody whom I work with, and I see him do something wrong, yeah, they will tell that is wrong."*

Individuals are happy to share knowledge with others in their team/department as well as with persons from other departments.

Regarding knowledge sharing within a department, participant (CY-R9) stated:

> *"I trust my colleagues, and the evidence for that is the fact that there isn't a significant amount of information that goes astray."*

Concerning trusting people from other departments and sharing knowledge with them, participant (CY-R4) said:

> *"...there is no particular restrictions on sharing knowledge with other departments. So we are quite open regarding sharing knowledge and obtaining knowledge from other departments."*

Knowledge sharing culture contains the trust of others, communication with others and the behaviour of the existing information system. During the investigation into the communication of information with others, this research found all the participants were satisfied with the processes of communication among individuals and teams within and outside their departments in the company. They are happy with the existing information systems in the company.

During the investigation of any cultural changes which could be effective for knowledge sharing for ID theft prevention in the company; the investigator found that there is no culture of knowledge sharing for ID theft prevention. The participants need a cultural change from top to bottom in the company for sharing the knowledge of ID theft. They require more training, education and awareness regarding ID theft issues and solutions to protect the organisational and personal information from fraudsters, along with a

computerised environment that could be used for sharing their knowledge for ID theft prevention.

Regarding the investigation of documents, the researcher found that the purpose of the policies was to keep risks to a minimum level. These documents include information about virus outbreaks, harassment, fraud, offensive and/or inappropriate content, company liability, personal responsibility, information leakage, excessive usage, unauthorised software, and unauthorised use of intellectual property rights. The documents showed that any hand-held device containing customer data should be issued by and owned by the company. Customer data should not be downloaded and stored on any of these devices which could be privately owned by individual staff members under any circumstances. It is the responsibility of the users to ensure that all hand-held devices were stored securely if they are taken off-site by following the company requirements.

If any equipment is lost or stolen outside company premises, the incident must immediately be reported to the police and the relevant department of the company. A crime reference number must be obtained from the police. If the device is lost or stolen on company premises, the incident must be immediately reported to the information security department of the company. Any delay in reporting such loss risks the potential for greater harm being suffered by the business.

The company uses a secure network. From the investigation of the documents, the researcher found that that the company provided and approved only devices from approved product vendors which could be connected to the networks which provide access to the core wired network. In the area of secure communication, the company follows standard protocols of secure transmission of data.

They have a dynamic and secure system of communication and data processing methods. The company has a training policy to enhance the knowledge of staff; however, from the analysis of the documents provided by *Company Y*, the researcher did not find any evidence of knowledge sharing for ID theft prevention in the company.

From the documents investigation and semi-structured interviews, the researcher found that the company has a secure IT infrastructure. They have policies for protecting the computers, secure network connections and communications. However, these documents do not include any policy on enhancing the knowledge of individuals and groups for ID theft prevention.

Table 5.5 Summary table for strengths, weaknesses and recommendations of *Company Y*

Factor	Strengths	Weaknesses	Recommendations
KM Infrastructure	- Uses different tools of knowledge sharing, for example, Share Point2007, email, e-learning system, and LYNC. - Individuals are happy with availability and usage of knowledge sharing tools.	- Knowledge sharing tools are not being used to share the knowledge for ID theft prevention.	- To use existing tools to share the knowledge for ID theft prevention. - Need to develop KM infrastructure to educate individuals and teams to share the knowledge for ID theft prevention.
ICT Know-how and Training	- The company provides departmental and company-wide induction. - Has scheduled training programs and refresher courses. - Provides training according to the job role of staff. - Arranges seminars to enhance the knowledge of the workers.	- Fundamental training on computers provided to the employees. - No training for ID theft prevention awareness. - Individuals and teams have a lack of know-how for sharing the knowledge for ID theft prevention in non-technical departments.	- Individuals need the know-how about ID theft issues. Non-technical departments require learning opportunities to enhance knowledge for ID theft prevention. - Develop knowledge sharing environment of ID theft prevention. - Enable process of education for staff to share their knowledge.
Job Rotation	- Very strong in job rotation process. - Individuals move from one department to another at their choice. - Individuals are enhancing their knowledge by working with others in different departments. - Teams get the advantage of staff whose job is being rotated in the new department.	- Jobs are not rotated for enhancing the knowledge of others for ID theft prevention in the company.	- Needs job rotation to increase the knowledge of ID prevention knowledge sharing.
Feedback on Performance Evaluation	- The firm impact of performance evaluation on individuals and teams. - Performance evaluation on departmental and organisational level. - The performance of employees is being evaluated for day-to-day routine work and feedback is being provided to them in one-to-one meetings.	- Performance is not assessed for ID theft prevention and its knowledge sharing. - There is no feedback for ID theft prevention knowledge sharing.	- Need to develop the culture of performance evaluation for ID theft prevention knowledge sharing and feedback may be provided to them.

Information Sourcing Opportunities	- Have internal network messaging system to share information in the company called 'Yammer'. - Use Microsoft SharePoint 2007. - Implemented centralised system called Connect. - Use emails to update staff. - E-learning system called e-portal on the website of the company. - PowerPoint presentations to the staff. - Has a library with a large amount of literature to enhance the knowledge of staff.	- Existing sources are not being used for ID theft prevention. - Do not have a policy of ID theft prevention. There is no use of existing opportunities for sharing knowledge for ID theft prevention.	- Need to focus on the usage of existing information sourcing opportunities for ID theft prevention knowledge sharing. - Set policy for the use of information sources to enhance the knowledge of individuals for ID theft prevention. - Enable teams and groups to use information opportunities for ID theft prevention awareness. - E-learning system could be enhanced as a source of knowledge sharing for ID theft prevention and increase the skill levels. More learning resources should be provided to the staff for ID theft prevention knowledge sharing.
Leadership Support	- The leadership of the company is very supportive. - Share information using email. - Leave general messages on Yammer. - Arrange meetings with subordinates. - Arrange seminars for staff awareness. - Staff are happy with management.	- Leadership is not motivating staff to enhance the knowledge for ID theft prevention. - The Knowledge sharing for ID theft prevention is not in focus of management of the company.	- A communication process for knowledge sharing for ID theft prevention. - Provide a learning environment for enhancing knowledge of ID theft issues and its prevention. - Leadership facilitate the staff with educating them about enabling knowledge sharing processes in different departments.
Knowledge Sharing Culture	- Teams get the advantage of knowledge sharing. Staff are trusted. - There is a culture of knowledge sharing outside of the department in the company. - Employees are happy with existing information system.	- There is no culture of knowledge sharing for ID theft prevention. - Individuals from non-technical departments have no awareness of how to share their knowledge for ID theft prevention.	- Need to develop the knowledge sharing culture for ID theft prevention.

The company has induction training programs for starters to provide them with information about working procedures and their job role (see Table 5.5), including training for computer usage at a basic level such as using databases, creating spreadsheets and sending and receiving emails.

At the moment the company has a policy for refresher courses to update their staff and arranges seminars to increase the knowledge of staff about their work. However, these

learning opportunities do not include enhancing the knowledge of ID theft prevention and its knowledge sharing. An advanced learning environment allows the staff to deal with the complex problems met. *Company Y* still needs to enable the staff of all departments to receive training regarding ID theft prevention practices. An e-learning system which they call an e-portal has been provided to update the staff regarding new events and other communication activities. The company uses an internal messaging system called 'Yammer'. For file sharing, they use Microsoft SharePoint 2007.

Table 5.5 summarises the findings in *Company Y* along with the strengths and weaknesses regarding sharing knowledge for ID theft prevention. In the company, the preferred method of communication is emailing, which is frequently used by staff. As discussed earlier, job rotation plays a vital role in increasing the knowledge of individuals and teams/groups. This study found a powerful process of job rotation.

Almost all the staff are transferred from one position to another. The participants were happy to learn from new departments and new staff members as they enhance their knowledge of different job roles through job rotation. However, the purpose of job rotation does not include enhancing their knowledge to understand the issues of ID theft and its prevention.

Therefore, the company needs to enhance the job rotation process to increase the knowledge of staff for ID theft prevention. Regarding the knowledge sharing culture, this research found a strong culture of knowledge sharing. Staff are trusted and share their knowledge with others outside their department in the company. However, the company needs to improve the culture of knowledge sharing for ID theft prevention.

The company, however, is not focusing on increasing the knowledge of individuals and teams for ID theft prevention. Staff require a knowledge sharing environment for ID theft prevention, and it is recommended that they utilise the current learning opportunities for enhancing knowledge sharing for ID theft prevention. It is also recommended that they develop a system for the knowledge sharing for ID theft prevention and the education of the workers in the process of knowledge sharing.

5.3.8. Existing Barriers in Knowledge Sharing for ID Theft prevention in *Company Y*

The present research study found the following barriers in knowledge sharing for ID theft prevention in *Company Y*:

- **Staff Unwillingness**

Individual staff willingness is essential in the process of knowledge sharing. Table 2.11 in the literature review chapter shows that a staff willingness for knowledge sharing is necessary for the organisation. The literature shows that being willing to share knowledge is one of the most important elements in the process of knowledge sharing for ID theft prevention in an organisation (see Section 2.5). The behaviour and attitude of individual staff members regarding knowledge sharing are beneficial to any organisation. Therefore, unwillingness is a barrier to knowledge sharing.

This study found that staff are willing to share their knowledge with others. A participant (CY-R03) said:

> *"If our company wants us to share the knowledge, I think we would be happy..."*

Another respondent (CY-R06) stated:

> *"People are always happy to tell you what they know. It is very much open."*

From the investigation of employee willingness for sharing the knowledge for ID theft prevention, this study found that staff members from non-technical departments were not aware of information protection and ID theft issues. However, they are happy to learn from others and share with others.

Participant (CY-R06) said:

> *"I do not know much about ID theft, but if anyone tells me about it, I will get it."*

This research study found that staff are willing to share knowledge with other staff members within and outside their department in the company. Therefore, staff unwillingness to share their knowledge for ID theft prevention is not a barrier in *Company Y.*

- **Lack of Staff Awareness**

The lack of awareness of individual staff members and teams regarding knowledge sharing can be a barrier in the process of knowledge sharing for ID theft prevention.

Individual employee awareness is essential for the success of the knowledge sharing processes in the organisation (see Table 2.12). Lee and Al-Hawamdeh (2002) state that acceptance of the significance of this would affect knowledge sharing between individuals, groups and teams in organisations. Employee awareness of the knowledge sharing processes encourages individuals to share their knowledge efficiently and provides the chance for creative thinking to handle complicated issues and understand the mistakes of others (Safa et al*.,* 2016). The literature clarifies that lack of staff awareness is a barrier to knowledge sharing and it needs to be managed accordingly (see Section 2.5).

However, the present study found a lack of awareness of sharing knowledge for ID theft prevention. From the supply chain department, participant (CY-R09) responded:

> *"I am not aware of identity theft. Well, I do not know about those problems."*

Another respondent (CY-R10) said:

> *"I have no idea about it. Nobody told me about identity theft."*

Regarding awareness of the use of technological tools for ID theft prevention, staffs from non-technical departments do not know about the availability and usage of existing tools for the knowledge sharing for ID theft prevention. Participant (CY-R06) responded that:

> *"I am not aware of the tools available for it."*

Interviewee (CY-R10) said:

> *"I do not know which identity type of systems they are using. No idea…"*

However, participants need awareness of ID theft issues identification and protection from these matters (CY-R07; CY-R08; CY-R10). Interviewee (CY-R08) responded that:

> *"I suppose just raise more awareness. Somewhere there are breaches of identity theft; we need it."*

From the investigation of internal documents research, no evidence was found for sharing knowledge for ID theft prevention. *Company Y* is not focusing on the awareness of ID theft prevention. There is a lack of staff awareness to share the knowledge for ID theft prevention. Therefore, it is a barrier in the process of the knowledge sharing for ID theft prevention in *Company Y*.

- **Insufficient Learning Opportunities**

An advanced learning environment enables workers to enhance their expertise to deal with complicated problems. Learning opportunities enhance progress by removing previous mistakes and weaknesses (Harteis et al., 2008). Various organisations provide various training opportunities for their employees to keep them up-to-date and to enhance the innovative techniques to improve performance. Table 2.13 describes the importance of the need for learning opportunities in sharing the knowledge for ID theft prevention in any organisation.

The present study found that *Company Y* has provided various learning opportunities to staff working in the company, for example, training for newcomers which they call induction, which is provided at departmental and company level. Other learning opportunities include group meetings at the team level, open days and various seminars for awareness for the staff (CY-R02). Employees are highly satisfied with the availability and usage of learning opportunities in the company. Moreover, current learning opportunities help them in their day-to-day jobs, communication with each other and the use of the current ICT environment.

However, currently, *Company Y* has no training program for ID theft prevention. When it was asked about the availability of the training for ID theft prevention, Participant (CY-R10) said:

> *"There is no mention of ID theft."*

Respondent (CY-R12) said:

> *"I do not think there is a specific training for that here that we receive."*

Participant (CY-R01) responded:

> *"There is no training for ID theft prevention in the company."*

As discussed earlier, a healthy learning environment plays a vital role in increasing the knowledge of employees for ID theft prevention. Staffs require an educational (learning) culture for the knowledge sharing for ID theft prevention in the company. Currently, the company emphasis is on the protection of customer information from fraudsters and ID thieves. Despite having various learning opportunities, staffs are not getting the advantage of enhancing their knowledge for ID theft prevention. Therefore, those learning opportunities are not being used for enhancing the knowledge of individual staff members

and teams in the organisation, and it is a barrier in the process of knowledge sharing for ID theft prevention in *Company Y*.

- **Distrust of Other Staff Members**

This research study found that staff trust each other and share knowledge within and outside their department in the company. While investigating the trust of others regarding sharing the knowledge for ID theft prevention, the researcher found that knowledge regarding ID theft prevention is not in the focus of the staff. However, individuals trust each other to share their knowledge about regular jobs and day-to-day activities in the company.

Participant (CY-R10) said:

> *"I trust people working there with me. I share knowledge with them. I would like to discuss anybody working here in the company. It will be helpful I consider it…"*

Staff are willing to share knowledge with people either in their department or who work in any other department in *Company Y.* Interviewee (CY-R09) said:

> *"I trust my colleagues, and the evidence for that is the fact that there isn't a significant amount of information that goes astray."*

Participant (CY-R04) said:

> *"There are no particular restrictions on sharing knowledge with other departments."*

Staff are trusted in *Company Y*. However, they are not sharing their knowledge of sharing for ID theft prevention. Therefore, *Company Y* needs to enhance the trust level for sharing the knowledge for ID theft prevention within the organisation.

- **Fear of Information Leakage**

Protecting information is a challenge for organisations; it's difficult to hide from the unauthorised access of fraudsters (see Table 2.15), and therefore, it is a major concern of the management of online retail companies; staff working in the organisations always fear information leaking into the wrong hands. Research studies emphasised various significant aspects of data leakage, which included insiders working in the organisations (see Section 2.5).

Therefore, companies are much stricter in the protection of their resources and data, which causes increasing the fear of information leakage outside the companies. *Company Y* has strict rules and regulations for the protection of information on the ICT infrastructure and information (CY-R02). Staff working in the company have confidence in the information security infrastructure, and they do not fear the leakage of information from outside attack on the IT systems in the company (CY-R13). Staff are trusted and share their knowledge with each other. Therefore, fear of information leakage is not a barrier in the process of knowledge sharing in *Company Y.*

- **Insufficient Information Sourcing Opportunities and Inefficient ICT Infrastructure**

The existing literature shows that an effective process of knowledge sharing needs well-structured information sourcing opportunities and an efficient infrastructure of ICT in any organisation; therefore, various organisations give importance to the availability of opportunities for information sourcing (Holsapple, 2013). Table 2.16 in the literature review chapter describes the need for sufficient information sourcing opportunities and an efficient ICT infrastructure for the knowledge sharing for ID theft prevention in an organisation.

Company Y has provided various information sourcing opportunities to its staff; for example, staff have access to the e-learning system which is called the e-portal in the company (CY-R01), and they use a messaging service called 'Yammer' (CY-R11), and employees access SharePoint, the emailing system, arrange seminars and street shows. The management update staff using PowerPoint presentations and a huge library exists in the company building which contains an enormous amount of literature for employees to enhance their knowledge (CY-R09; CY-R11).

Regarding the investigation of internal documents, the researcher found that the company has taken proper measures to secure the information of the organisation and its customers. The participants were happy with the availability of the ICT infrastructure. Respondent (CY-R12) said:

> *"I am pretty satisfied because the way the IT systems work here, there are quite a lot of checks and balances in place which will avoid such a problem."*

The staff have various information sources to update their knowledge but the company is not focusing on the awareness of ID theft issues, and its prevention and individuals and teams are not getting the advantage of using this information sourcing.

Participant (CY-R03) said:

> *"The various tools we use, are user point. But I do not think it is for prevention of identity theft."*

Therefore, the present study found that the current information sourcing opportunities and ICT infrastructure are not being used for the processes of the knowledge sharing for ID theft prevention in the organisation. Therefore it is a barrier to knowledge sharing for ID theft prevention in *Company Y*.

- **Lack of Leadership Support**

According to Muethel and Hoegl (2016) and Bass and Stogdill (1990), the leadership of any organisation plays a vital role in managing the processes of knowledge sharing. It is, therefore, their responsibility to practice strategic planning for the best use of resources and to enhance the learning culture and knowledge sharing in any organisation (Boerner et al., 2007). The leadership is required to bring about an open culture and to build the environment for knowledge sharing (Chuang et al*.,* 2016) and therefore, for top management to give support to articulate the value of knowledge sharing. They should provide this to signify knowledge sharing approaches in the organisation (Mittal & Rajib, 2015).

The management of *Company Y* is supportive, and they share information with staff in different ways. Managers make conversation with staff members through email contact. Respondent (CY-R01) said:

> *"My concerned managers send me emails about the issues and about my work I do here."*

Managers also arrange sessions for group discussion to discuss the working tasks and guide the staff members. Participant (CY-R05) stated:

> *"We arrange a session to discuss staff and help them with work."*

This research study found that middle management gives instructions to staff through group meetings (CY-R10); they see employees in one-to-one meetings and listen to them about the facilities available to them and any further requirements of work in the

organisation (CY-R09). Management also arranges conferences and seminars for employee awareness.

For the investigation for the support of leadership in the knowledge sharing processes and enhancing the knowledge of individuals and teams in the company, the researcher found that currently, management is not focussing on the knowledge sharing processes for ID theft prevention in the organisation. From the investigation of internal documents of the company, the present study found that the leadership is supportive and helpful in securing the IT infrastructure and information of organisation and customers. However, the research did not find any evidence for the process of enhancing the knowledge of individual staff members and the organisation in the context of ID theft prevention and process for it.

There is a lack of leadership support for sharing the knowledge for ID theft prevention, and it is a barrier to the process of the knowledge sharing for ID theft prevention within the organisation.

- **Weak Knowledge Sharing Culture**

According to McDermott and O'Dell (2001), the organisational culture is the combination of shared values, beliefs and performances of employees in any organisation. It is one of the main elements considered in any organisation for knowledge sharing between individual staff members and teams in the organisation (see Table 2.18). Knowledge sharing can work if the culture of the organisation supports it, and changes need to be developed according to the culture of the organisation (Stoddart, 2001), and therefore this needs to be understood in advance before employing new strategies in the organisation. A weak culture of knowledge sharing causes an obstacle to the process of knowledge sharing in the organisation so that it needs to be managed for the effective knowledge sharing processes in the organisation.

Company Y has a strong culture of knowledge sharing. Staff members are trusted, and they share knowledge with each other in the department.

Participant (CY-R06) said:

> *"I trust my friends. Actually, we help each other in our department."*

On the other hand, the researcher found that there is a culture of knowledge sharing between employees at intra-departmental level. Staff trust other employees working outside their department (CY-R01; CY-R10). Another participant (CY-R08) said:

> *"We have a good culture of information sharing. We are quite good in trust of others. Well, I can trust all staff here working in this company, and I should do it as others trust me."*

Individual staff members are willing and happy to share knowledge with others in their team or department and with the persons of another department.

However, this study did not find a culture of the knowledge sharing for ID theft prevention. Staff are not sharing their knowledge regarding ID theft prevention, and therefore it is a barrier to the process of knowledge sharing for ID theft prevention in *Company Y*.

- **No Job Rotation**

Job rotation plays a vital role in increasing the knowledge of individual members and teams within and outside any department in any organisation (Aga et al., 2016; Huang & Pan, 2014; Ortega, 2001). Table 2.19 describes the advantages of job rotation for increasing the knowledge of employees in the organisation. It is useful for employee learning as employees learn while working with new staff members in different teams or departments; they also learn from the new environment and new types of work. It is also useful for employer learning, as due to the job rotation of employees, employers learn about the weaknesses and strengths of individuals working in the organisation.

The researcher found *Company Y* very strong in the process of job rotation. Staff members are getting the advantage of job rotation for increasing their knowledge while working in different teams and departments in the company (CY-R08). They learn about new systems which were not used in the previous departments and learn from the experiences of other departments (CY-R06). Staff are happy and also learn methods of doing something different with the new job role and experience new things. Participant (CY-R13) said that:

> *"I am happy to work with the new environment and new people. I learn from them, and it leaves me no chance of failure. So I am happy with it."*

Respondent (CY-R12) said:

"It is just by gaining knowledge of different areas."

Concerning the usefulness of job rotation for increasing the knowledge of employees for prevention of ID theft in the company, however, the company is not rotating the jobs to increase the knowledge of persons for ID theft identification and its prevention. Therefore, job rotation does not play a role in enhancing the knowledge of individuals in the company for ID theft prevention. The departments are not getting the advantage of the knowledge sharing for ID theft prevention from the people of other departments.

Table 5.6 Barriers to knowledge sharing for ID theft prevention in *Company Y*

S.No	Barrier in KS for ID theft prevention	Empirical Findings in *Company Y* (Barrier in KS for ID theft prevention)
1	Staff unwillingness	No
2	Lack of individual staff awareness	Yes
3	Insufficient learning opportunities	Yes
4	Distrust of other staff members	No
5	Fear of information leakage	No
6	Insufficient information sourcing opportunities and inefficient ICT infrastructure	Yes
7	Lack of leadership support	Yes
8	Weak knowledge sharing culture	Yes
9	No job rotation	Yes

Not rotating jobs to increase the knowledge of individuals and teams to enhance the knowledge of ID theft identification and its prevention leaves the individuals to learn from their own experiences. Therefore it is a barrier to the knowledge sharing for ID theft prevention in the organisation. The lack of job rotation causes no enhancement of the knowledge of individuals and teams in the organisation.

Table 5.6 describes the barriers in the knowledge sharing for ID theft prevention in *Company Y.* This study found that staff were willing to share knowledge with others in the company. Therefore, staff unwillingness is not a barrier in *Company Y*, as staff are willing to share their knowledge in the company. However, there is a lack of awareness of workers regarding knowledge sharing in the company.

Individuals working in non-technical departments are unaware of ID theft issues and protection from these problems, and therefore it is a barrier to knowledge sharing for ID theft prevention in the company. Available learning opportunities are insufficient to

enhance the knowledge of staff working in the company, which causes not sharing knowledge. Staff members are trusted and are willing to share their knowledge with other employees working in their department as well as in other departments. There is no lack of trust in individuals and teams from different departments. Therefore, distrust of other staff members is not a barrier.

Due to having the trust of other workers in the company, individual staff members do not have a fear of information leakage. There is no culture of knowledge sharing for ID theft prevention in *Company Y*. The existing ICT infrastructure and information sourcing opportunities are not capable of sharing the knowledge for ID theft prevention between individuals and teams in different departments of the company, and it is a barrier to knowledge sharing for ID theft prevention. The leadership of the company is very supportive; however, there is no support by the leadership to enhance the knowledge of individuals to share their knowledge for ID theft prevention in the company. The researcher found *Company Y* very strong in the process of job rotation. However, the purpose of job rotation is not enhancing the knowledge of individual staff members and teams to share their knowledge of ID theft prevention. Therefore, it is a barrier to the process of knowledge sharing for ID theft prevention in *Company Y*.

5.4. Knowledge Sharing Processes for ID Theft Prevention in *Company Z*

For the data collection of the third case study, the researcher contacted a large number of companies; it was found to be almost impossible to get access to a third company to collect data. However, after a long struggle, a response was received to conduct a small case study of four to seven interviews in *Company Z.* The company provided seven interviews with its employees working in both technical and non-technical departments. All interviews were face-to-face in Company *Z.* Table 5.7 shows the list of participants in *Company Z.* Data collection also included internal documents from the company.

The company provides services and consultancy to retailing companies and their customers. Since it started in 2008 as a contact centre, they have supplied services and consultancy to more than 200,000 client companies and customers. The philosophy of the company is *"send the right message to the right person",* which is what makes them different. They take the time to understanding clients' sales strategies and then execute them at the highest level of consultancy through telephonic and direct email contacts. The

company is expert at taking new products to the market and enhancing awareness among prospects. It provides the services of outbound sales, inbound sales, customer services, customer retentions and maximises the revenue of the client companies and customers.

Table 5.7 List of interview participants in *Company Z*

Participant Code	Position of Participant	Participant Department	Participant Job Responsibility	Participant Experience	Interview Duration
CZ-R01	System Administrator	Information Technology	Managing the website of the company, updating web contents. Handling the database at backend.	7 years	53 mints
CZ-R02	Network Manger	Information Technology	Look after IT infrastructure, administrating existing system including the network and hardware in the company.	5 years	50 mints
CZ-R03	Information Security Consultant	Information Security	Handling information on security issues of the company. Managing firewalls and secure lines for the company.	5 years	65 mints
CZ-R04	Customer Service Advisor	Call Centre	Contacting the customers. providing sales advice.	3 years	46 mints
CZ-R05	Customer Service Advisor	Call Centre	Contacting the customers. providing sales advice.	1 year	47 mints
CZ-R06	Regnal HR Manger	Human Resources	Managing human resources in the company.	7 years	53 mints
CZ-R07	Customer Service Advisor	Call Centre	Contacting the customers. providing sales advice.	3 years	46 mints

This research study found that the sales agents are trained to the highest degree, with the best product knowledge, superb closing skills and up-selling techniques that leave the customer highly satisfied. Their agents are trained to understand customer psychology; they know that every call and caller is unique and should be treated as such. They have a policy of ‘listen twice as much as customers speak’ so that the customer service advisor fully understands the customer’s problem, verifies the problem and gives the customer all the possible solutions. They do not take customer service lightly because they understand the cost of initial acquisition and that it is far better and easier to excel at customer service to maintain a customer’s continued and loyal patronage.

5.4.1. KM Infrastructure

For the investigation of KM infrastructure in *Company Z,* the researcher found that the company uses tools to share knowledge among the staff which include Yammer, email and an e-learning system and the policy documents which are uploaded to the website of the company (CZ-R06; CZ-R07). The present study found that all the participants were satisfied with the availability of the knowledge sharing tools. Participant (CZ-R01) said:

> *"I am happy what I got here."*

Interviewee (CZ-R02) responded:

> *"We have strong tools to share the knowledge of what we do."*

They are happy with the existing tools to share their knowledge. On the other hand, staff members do not use these tools for sharing knowledge for ID theft prevention.

Participant (CZ-R03) said:

> *"I'm really happy with IT systems available here; there are so many layers which help to avoid security issues. And we have good knowledge sharing system too. But these systems are not used for ID theft prevention."*

Regarding the skills required for sharing the knowledge for ID theft prevention, the participants from the call centre of the company require training to enhance their awareness for such type of issues and how to share that knowledge with other staff members within the company.

Respondent (CZ-R04) from the call centre said:

> *"I don't know about ID theft problems. I need help in it. I deal with the customers, and it will be helping for me if I had some knowledge of those issues and needed to protect my personal information."*

Interviewee (CZ-R07) reported:

> *"I require awareness for it. If company arrange some training and some seminars…"*

The participants are happy with the existing KM infrastructure. The resources required for routine jobs are available to staff, and they are satisfied with the usage of the existing resources, but for sharing the knowledge for ID theft prevention, staff demand awareness of ID theft issues and how to protect against them.

5.4.2. ICT Know-how and Training

Company Z is very good at providing training for staff members working in the company. All staff have been trained when newly joining the company, which is called induction. The company has a policy of scheduled training. Furthermore, staff are offered various refresher courses from time-to-time.

They have a policy of company-wide training as well as departmental induction training. The company-wide induction introduces the infrastructure of the company, which includes the available resources, culture, and the environment of the company. During the departmental inductions, newcomers are introduced to the departments, the working procedures and the existing information systems in the company. Departmental induction also includes training sessions with information about their job role.

Participant (CZ-R02) responded:

> *"When I joined the company they provided training about the infrastructure, the way I work and how to deal with others in groups or in the working environment."*

Participant (CZ-R05) said:

> *"At first they trained me a lot, you know. They introduced me how to use the system, how to deal with our customers."*

The company provides training to the employees as per the requirements of the usage of the existing resources. The researcher found that staff have been trained at a basic level to use the IT resources such as at the level of information about using the computers and the software tools for their routine working activities (CZ-R04; CZ-R05).

The company has a scheduled training policy, which includes quarterly, semi-year and yearly training. This training is provided to the staff to keep their knowledge up-to-date according to their work (CZ-R6).

The company provides training which includes ID theft prevention to the information Technology and Information Security Department. A participant (CZ-R02) from the IT department responded:

> *"We have training for how to secure the systems, and yes, I had a session for ID theft during the IT security training."*

While investigating any training available for the knowledge sharing for ID theft prevention, the researcher found that knowledge for ID theft prevention is not being shared among individuals. From the responses of the reasons for not providing training for sharing the knowledge for ID theft prevention, this study found that staff members are unaware of the sharing of such type of knowledge. Participant (CZ-R04) responded:

> *"I don't know how to share ID theft knowledge. It is not my concern."*

Participant (CZ-R05) said:

> *"I never use it, and nobody told me about it."*

This research found that there is no policy for sharing knowledge for ID theft prevention; at the moment company is not focusing on enhancing the knowledge of individuals as well as teams/groups for prevention of ID theft within or outside their department of the company.

5.4.3. Job Rotation

During the investigating the process of job rotation, the researcher found that the company has no policy of job rotation for the sake of enhancing the knowledge of staff.

Participant (CY-R05) said:

> *"I don't know about the job rotation."*

Interviewee (CZ-R06) responded:

> *"We do not have any policy of job rotation in the company here."*

Staff are learning from their own experiences. Respondent (CZ-R02) said:

> *"I gain knowledge from my things I experience here, and I do not need to go anywhere and ask how to do my work."*

According to participant (CZ-R03), people are not moved from one seat to another seat and from one department to another department unless they get promoted to the next job. While asking the reason for not rotating the jobs of staff, participant (CZ-R06) said that:

> *"Our staff are very experienced in their work, and they do not need to work in other environments of any department of the company."*

Individuals and teams/groups are not getting any advantage from other experienced staff members in the company. The company is not rotating the jobs of staff members to enhance their knowledge for the prevention of ID theft. Therefore, this research recommends that they implement the process of job rotation so that individuals and teams can get the advantage of enhancing their knowledge for ID theft prevention in the company; they also can learn from the experiences of the staff moved from other working areas of the company who has expertise in ID theft prevention.

5.4.4. Feedback on Performance Evaluation

The company has a policy of one-to-one meetings with staff members once a month. During these meetings, departmental managers and staff members discuss the tasks performed during the month. At the end of the meetings, the managers provide feedback to the staff about the activities completed.

Participant (CZ-R04) said:

> *"We meet every month. My manager asks me about the job I did during the months. And he writes everything discussed in the meeting."*

The company has a policy of evaluation of employees once a year. All staff members fill in an online evaluation proforma which is placed on the website of the company. The management of the company provides feedback to the staff by processing the online evaluation proformas. Participant (CZ-R06) said:

> *"Our method of filling evaluation forms online make us easy to access the staff and we easily calculate their work and provide them feedback on the basis of results we get from that process."*

At the end of the year, all staff are bound to fill in hard copy appraisals which go through the departmental management to top management (CZ-R02). In the appraisals, managers provide remarks about the staff, about their behaviour with other members and with the managers, and how they have performed their work in the company.

Feedback is provided on the basis of work activities, the tasks completed and the behaviour of the staff with other members of the department or team. These meetings take place in a separate room and during the meetings the relevant managers give feedback to the staff. The company evaluates the performance of employees twice, as in *Company Y*.

Every staff member needs to fill in a pro forma that they call an appraisal (CZ-R01; CZ-R05).

This study found that the company is not evaluating the performance of employees for knowledge sharing for ID theft prevention. While investigating the reason for not evaluating the performance of staff in the context of the knowledge sharing for ID theft prevention, the participants responded that they do not share the knowledge of ID theft prevention and that is why there is no need for evaluation of it. Therefore, there is no impact on the performance evaluation of employees on it.

At the moment the company does not have any system for evaluating the performance of staff for sharing the knowledge of staff, and they are not getting any feedback in this context. The company needs to evaluate the individuals and teams and groups for knowledge awareness and to know at what level the staff are updated regarding ID theft issues and its prevention.

5.4.5. Information Sourcing Opportunities

The company has made available different information sourcing opportunities to the staff which include Yammer, email and policy documents. The participants responded that knowledge is being shared through emails (CZ-R06) and chat in Yammer. The company website holds policy documents which provide information to the staff about the working environment and about the rules and regulations of the company (CZ-R02; CZ-R07).

Staff prefer to use email as their preferred source for knowledge sharing. The reason for their preference to the usage of email for sharing the knowledge is that it can be easily accessed anytime.

Participant (CZ-R06) responded:

> *"I prefer email because I can receive it anytime. I can read it and reply to sender very quickly."*

Participant (CZ-R02) said:

> *"My manager send me email that what things to do and when to do."*

According to all participants, email is the main source which provides the most up-to-date information to them. Staff are happy with the availability of information sourcing opportunities which they use for communication. On the other hand, this study found that

those available information sourcing opportunities are not being used for the knowledge sharing for ID theft prevention in the company. Therefore it is recommended to facilitate the individuals as well as the teams and groups with opportunities for sharing the knowledge for ID theft prevention.

5.4.6. Leadership Support

The leadership of *Company Z* is very helpful, and they use different ways to disseminate information among the staff of the company. According to the participant (CZ-R06), the management provides all the facilities to the staff required to work in the company. Interviewee (CZ-R01) said:

> *"Whenever we require something we ask our managers and they arrange for it. Sometimes my manager comes down and asks us if we require something."*

While asking the management about the methods of knowledge sharing from them, the researcher found different ways in which managers share information with their subordinates and staff members working in the company. For example, they send group emails to others to update them. The line managers call group meetings and discuss the problems and working activities (CZ-R02; CZ-R04; CZ-R07).

The communication between leadership and staff includes discussion about information security issues and about cyber security problems (CZ-R03). However, that communication does not include sharing the knowledge of ID theft among individuals and groups/teams within or outside the departments in the company (CZ-R01).

Staff are expecting support from the leadership of the company for knowledge awareness for ID theft issue and its prevention. They need the guidance and education for ID theft issues and how to prevent it and how to protect personal and organisational knowledge from unauthorised persons.

5.4.7. Knowledge Sharing Culture

Company Z has a good knowledge sharing culture at the departmental level. Staff trust each other within their departments. They happily share knowledge with others in their own department.

Participant (CZ-R01) said:

> *"I trust my friends who work with me. We work together and support each other to maintain the system and provide IT facilities in the company."*

Interviewee (CZ-R02) responded:

> *"I trust them because they work with me and we need to share our work information. We are the security department we must help each other and secure the systems here."*

When it was asked whether they trust others outside the department, most of the participants responded that they do not trust those with whom they do not work. Staff are reluctant to share knowledge with others outside the department. Therefore, the researcher found that departments are not getting the advantage of knowledge sharing outside the department. While asking about sharing the knowledge for ID theft prevention, participant (CZ-R03) responded that:

> *"I do share ID theft knowledge with my friends who work with me, but I do not share such type of information with the people I am not working with."*

Individuals and teams/groups get the advantage of sharing knowledge of information security and ID theft prevention in information technology and information security departments; however, staff from non-technical departments need to enhance their trust level, and they need to be educated to enhance their knowledge of ID theft prevention.

Table 5.8 summarises the findings of knowledge sharing processes for ID theft prevention in *Company Z,* showing the strengths and weaknesses of the company. This study also recommends solutions for enhanced knowledge sharing processes for ID theft prevention in the company.

Table 5.8 Summary table for strengths, weaknesses and recommendations in *Company Z*

Factor	Strengths	Weaknesses	Recommendations
KM Infrastructure	- The company has knowledge sharing tools, such as Yammer, email and e-learning system. Policy documents uploaded on the website. - Satisfactory KM infrastructure.	- Knowledge sharing tools are not being used for ID theft prevention. - Individuals and teams are not getting advantage from existing tools to enhance the knowledge for ID theft prevention.	- The environment is needed for knowledge sharing for ID theft prevention. - Staff need to enhance information skills about ID theft issues and to protect organisational and personal information.
ICT Know-how and Training	- Departmental level and company-wide induction. - The policy for the training schedule. - Availability of refresher courses and seminars to enhance knowledge. - ID theft prevention training for staff from information security department.	- Basic training on IT infrastructure and computers. - There is no policy of ID theft prevention knowledge sharing to other departments. - Lack of know-how of ID theft issues to non-technical staff.	- Require training on ID theft prevention and its knowledge sharing to employees of departments other than IT department. - Enhance the educational process for knowledge sharing. - Requires the development of knowledge sharing system for ID theft prevention.
Job Rotation	- No job rotation.	- There is no job rotation at all.	- To implement the process of job rotation of individuals and teams/ groups to enhance the knowledge of ID theft issues and its prevention.
Feedback on Performance Evaluation	- Provides feedback on a monthly basis. - Staff go through performance evaluation every month. - The performance of the employees is being evaluated as per working activities and given feedback on results.	- No performance evaluation process for knowledge sharing for ID theft prevention. - No feedback for ID theft prevention knowledge.	- Staff evaluation is required for the knowledge level of staff for ID theft prevention awareness.
Information Sourcing Opportunities	- Uses an internal messaging system called 'Yammer'. - Provides policy documents to the staff. - Email communication.	- Information sourcing opportunities are not being used for the knowledge sharing for ID theft prevention	- To facilitate the individuals and teams/ groups for opportunities for sharing the knowledge for ID theft prevention.
Leadership Support	- Helpful and supportive leadership. - Share knowledge via meetings, emails and phone calls.	- Not focused on increasing the knowledge of staff for ID theft prevention and to share its knowledge.	- Leadership support is required implementing a knowledge sharing environment for ID theft prevention.

Knowledge Sharing Culture	- Has knowledge sharing culture at the departmental level. - Staff are trusted at the departmental level in the company. - The knowledge is being shared for ID theft prevention in IT and information security departments.	- Knowledge is not being shared outside the department in the company. - Staff from other departments are not trusted. - No culture of the knowledge sharing for ID theft prevention. - Only two departments have a culture of knowledge sharing for ID theft prevention.	- Staff from non-technical departments need to enhance their knowledge for ID theft prevention. - The enhanced trust level is needed in non-technical departments.

This research found that the company has provided various opportunities for ICT know-how and training to the staff. All staff joining the company go through training they call induction. They have a policy of scheduled training, and the company arranges seminars to enhance the knowledge of staff in the company. However, these learning opportunities do not include the enhancement of knowledge of individuals and groups/teams to prevent ID theft and share its knowledge to update others. At the moment, the company does not have a policy for knowledge sharing processes for ID theft prevention. A strong knowledge sharing environment in the organisation requires enhanced information sourcing opportunities. The company has provided information sourcing opportunities which include the company's internal database, the internal network messaging system (Yammer) for staff communication, an email communication system and policy documents uploaded on the website. However, these opportunities are not being used for knowledge sharing for ID theft prevention in the company.

Job rotation plays a vital role in enhancing the knowledge of individuals and teams, who have the opportunity to learn from the others' experiences while working in a new environment in the job rotation process.

This study found that there is no job rotation process in *Company Z;* staff are learning from their own experiences. Therefore, the company needs a job rotation process to enhance the knowledge of individuals and people working in teams. Regarding feedback on performance evaluation, the researcher found that the company has a policy of evaluating the working process and providing feedback to staff on a monthly basis. Furthermore, all staff members go through the evaluation process once a year at the company level.

However, the company does not evaluate the knowledge level of staff for awareness for ID theft and its prevention. Staff evaluation is required for the knowledge sharing for ID theft prevention in the company; therefore it is recommended that the company develops an evaluation process. Leadership is very supportive in the company, and they fulfil all the requirements of the staff whatever they need in the working environment. The management of the company communicates with individuals and departments via email. They also arrange meetings and use telephonic contacts to communicate and share information with others. However, the researcher did not find any evidence of the knowledge sharing for ID theft prevention by the management of the company.

In respect of a knowledge sharing culture, this study found that the company has an adequate knowledge sharing culture at the departmental level. Staff are sharing knowledge and are trusted within their departments. Employees from IT and the information security departments share knowledge with each other in their departments, while staffs from non-technical departments are not trusted. Therefore, the company requires a trust level in non-technical departments to provide awareness for ID theft issues and its prevention. The company has a good KM infrastructure. However, the company needs to enhance the knowledge sharing processes for ID theft prevention.

5.4.8. Existing Barriers in Knowledge Sharing for ID Theft Prevention in *Company Z*

This research study found the following barriers to knowledge sharing for ID theft prevention in *Company Z.*

- **Staff Unwillingness**

The literature shows that the process of knowledge sharing depends on the willingness of individual staff members working in the organisations. The argument of Robertson and O'Malley Hammersley (2000) clarifies that staff who have satisfaction in their jobs and commitment to their companies are willing to share their knowledge; they believe in the advantages of the organisation as their benefits. The literature describes the importance of the willingness of individual staff members to share their knowledge in any organisation (see Table 2.11). Therefore, the willingness of staff to share their knowledge for ID theft prevention is mandatory and leads the online retail organisation to be knowledge oriented about ID theft prevention.

Individual staff members in *Company Z* are willing to share their knowledge within their department. Participant (CZ-R01) responded that:

> *"I am happy to discuss with my friends work here, but I will not share any knowledge outside this department."*

Staff from the technical department are not willing to share knowledge with others at intra-departmental level (CZ-R03).

However, workers in a non-technical department are happy to share their knowledge with individuals and teams.

Participant (CZ-R06) from the human resources department said:

> *"I can share knowledge with others and help them with the work."*

However, the management of the company is not focusing on the willingness of individual staff members to share their knowledge for ID theft prevention. Therefore, it is a barrier to the knowledge sharing processes for ID theft prevention in the company.

- **Lack of Individual Staff Awareness**

Individual staff members' awareness of the knowledge sharing processes is mandatory in an organisation. Employee awareness of the knowledge sharing processes encourages the individual staff members to share their knowledge effectively and provides the chance for creative thinking to handle complicated issues and understand the mistakes of others (Safa et al., 2016). The literature clarifies the need for individual staff awareness of knowledge sharing (see Table 2.12).

Staff working in the IT department and the information security department of *Company Z* are aware of the severity of ID theft and its impact on business and customers. Participant (CZ-R02) said:

> *"I am aware of identity theft issues and to protect from those."*

Respondent (CZ-R03) said:

> *"We had training about cyber security and information security. It included identity theft. Yeah, I am aware of it."*

However, staff working in a non-technical department, such as the HR department and the Call Centre, are not familiar with ID theft issues and how to protect against them (CZ-R05; CZ-R06). For the knowledge sharing processes for ID theft prevention, individuals

are unaware of the processes of knowledge sharing in the organisation. From the investigation of the internal documents of *Company Z,* the researcher did not find any evidence of enhancing the knowledge of individuals for sharing the knowledge for ID theft prevention. There is a lack of individual awareness in sharing the knowledge for ID theft prevention, and it is a barrier in *Company Z.*

- **Insufficient Learning Opportunities**

There is a strong role of learning opportunities in enhancing the knowledge of individuals working in any organisation. Table 2.13 shows the need for learning opportunities in knowledge sharing in an organisation. This study found that *Company Z* has a strong environment for training as almost all staff are being trained in the company. It has a policy of departmental and organisational level training for staff members joining the company which includes know-how about the working environment and the IT infrastructure. The company has a scheduled program of training and additionally, employees avail themselves of different refresher courses from time-to-time.

The company provides training on ID theft prevention to the staff members from the information technology and information security departments.

Respondent (CZ-R02) said:

> *"We have training for how to secure the systems, and yes, I had a session for ID theft during the IT security training."*

However, staff members from non-technical departments do not have access to any learning opportunities to enhance their knowledge for ID theft prevention.

Participant (CZ-R04) said:

> *"I do not know how to share ID theft knowledge. It is not my concern."*

Interviewee (CZ-R05) responded:

> *"I never use it, and nobody told me about it."*

Even though this research found that there is no policy for sharing the knowledge for ID theft prevention, at the moment the company is not focusing on enhancing the knowledge of individuals or teams for ID theft prevention within or outside the departments of the company. Therefore, a lack of learning opportunities is a barrier in the knowledge sharing for ID theft prevention in *Company Z.*

- **Distrust of other Staff Members**

Trust of other staff members is a fundamental element of knowledge sharing in any organisation. Table 2.14 shows the need for the trust of others in knowledge sharing. According to Pervaiz et al. (2016), trust and sincerity can support a vigorous knowledge sharing performance through successful communication promptness by providing a mandate to the members of organisations for sharing the knowledge that they possess.

Employees in *Company Z* have the trust of others within their department. They share knowledge with others working individually and in teams within the departments (CZ-R02; CZ-R06). However, staff working in the technical departments do not trust the staff of non-technical departments (CZ-R01; CZ-R03). Therefore, there is a lack of trust in *Company Z,* and it is a barrier to the process of the knowledge sharing for ID theft prevention in the company.

- **Fear of Information Leakage**

The fear of information leakage is an obstacle to knowledge sharing. Leakage of information can have various impacts on organisations, for example, loss of revenue, reputational damage, loss of productivity, and costs arising from breaches of agreements of confidentiality in the organisations. With huge compensation struggles, the organisations can recover from such problems. However, employees working in the organisation have a fear of information leakage while sharing it with others (see Table 2.15). Therefore, they are reluctant to share information security knowledge, especially ID theft prevention knowledge. As a result, it causes not sharing knowledge in the organisation and is one of the knowledge sharing barriers which need to be removed for the effective process of knowledge sharing in organisations.

From the investigation of internal documents in *Company Z*, this study found the company has strong rules and regulations concerning information security. Staff working in the company are strictly bound to the secure use of IT resources. Therefore, it causes fear of information leakage to the staff members working in the company. Participant (CZ-R02) said:

> *"I do not trust others. Anybody can leak the information. That is why we do not share security knowledge."*

Another respondent (CZ-R03) responded:

"People are not trusted, they can steal information, I am afraid to share security knowledge."

The fear of information leakage is a barrier in *Company Z,* and it impacts on the knowledge sharing for ID theft prevention in the company.

- **Insufficient Information Sourcing Opportunities and Inefficient ICT Infrastructure**

The literature includes the importance of having sufficient information sourcing opportunities and an efficient ICT infrastructure for sharing the knowledge for ID theft prevention in the organisation. Table 2.16 in the literature review chapter describes the need for information sourcing opportunities and an efficient ICT infrastructure in knowledge sharing.

The present study found that *Company Z* has numerous information sourcing opportunities such as a corporate conversation messenger they call 'Yammer', emails and policy documents (CZ-R03; CZ-R06). The company website also holds policy documents which provide information to the staff about the working environment and the rules and regulations of the company. Participant (CZ-R07) said:

"We have policy documents on the website."

All participants consider email to be the main source of information receiving in the company that provides up-to-date information to them.

Participant (CZ-R04) responded:

"I send and receive many emails a day, and I am happy with the use of email here in this company."

Staff are satisfied with the availability of information sourcing opportunities in the business. However, the present study found that the available information sourcing opportunities are not sufficient for the knowledge sharing for ID theft prevention in the company, and even the current opportunities are not being used for the knowledge sharing for ID theft prevention.

While talking about the ICT infrastructure, this study found a good infrastructure for securing the information and information assets in the company. From the investigation of the internal documents, the researcher found that the company has a strong policy for securing the information of customers and the organisation, including strong rules of

usage of the IT infrastructure and the communication system. The participants responded that they do not use the ICT infrastructure for disseminating the knowledge for ID theft prevention between various departments in the company. The existing ICT infrastructure is not efficient for the knowledge sharing for ID theft prevention, and therefore it is a barrier to the knowledge sharing process for ID theft prevention in *Company Z.*

- **Lack of Leadership Support**

The leadership of any organisation plays a major role in enhancing the knowledge sharing process in the organisation. Table 2.17 describes the literature covering the need for the support of leadership in the process of knowledge sharing in any organisation and the leadership required to bring about an open culture and to build the environment for knowledge sharing (Chuang et al., 2016).

The leadership of *Company Z* is helpful; they use different methods of communication with individual staff members and departmental managers in the company. The management of the company provides the employee with the required resources (CZ-R06). Participant (CZ-R01) said:

> *"Whenever we require something we ask our managers and they arrange for it."*

The communication between leadership and staff also includes information on security issues and cyber security problems (CZ-R02; CZ-R03). However, that conversation does not contain the awareness of individuals and teams about ID theft issues, its prevention and the process of knowledge sharing; staff from the non-technical departments are not aware of the ID theft issues and protection from these matters. The company leadership does not even have a policy for enhancing the knowledge for ID theft prevention in the company. There is no leadership in support of the processes of knowledge sharing for ID theft prevention in the company, and it is a major barrier in knowledge sharing for ID theft prevention.

- **Weak Knowledge Sharing Culture**

According to Stoddart (2001), knowledge sharing can work if the culture of the organisation supports it, and changes need to be developed according to the culture of the organisation. A weak culture of knowledge sharing causes hurdles to the knowledge sharing processes. Table 2.18 describes the need for knowledge sharing culture in an organisation. Therefore, it needs to be managed for an effective knowledge sharing process in the organisation.

Company Z has a culture of knowledge sharing at the departmental level. Participant (CZ-R01) said:

> *"I share what I do here in my department. Others also do it."*

However, they do not share knowledge with staff members working outside their department.

Respondent (CZ-R07) said:

> *"I do not know about the knowledge sharing. I do not do it. We do not discuss with others who do not work with us."*

The company does not have a knowledge sharing culture to enhance the knowledge for ID theft prevention within the company.

Interviewee (CZ-R03) said:

> *"We are not sharing such type of knowledge. We do not have instruction for it."*

There is no culture of the knowledge sharing for ID theft prevention in *Company Z,* and it is a barrier.

- **No Job Rotation**

Currently, *Company Z* is not rotating the job of individuals. From the investigation of internal documents, the research did not find any evidence of a job rotation process in the company. During the interview, participants said that their jobs are not being rotated. Interviewee (CZ-R06) responded with the words:

> *"We do not have any policy of job rotation in the company here."*

Staff are learning from their own experiences.

From the responses of the participants, the researcher found that staff are learning from their own experiences and doing the same jobs after years of working in the company. Respondent (CZ-R02; CZ-R06; CZ-R07) said:

> *"I gain knowledge from my things I experience here, and I do not need to go anywhere and ask how to do my work."*

The literature clarifies that job rotation is essential for enhancing the knowledge of employees to prevent ID theft and share the knowledge for ID theft prevention (Kane et al*.,* 2005). Table 2.19 shows that job rotation increases the knowledge of individuals, and

enables employers to find the employees' strengths and weaknesses. Therefore, a lack of job rotation causes not enhancing the knowledge of individuals and teams in the organisation in *Company Z*. Not rotating jobs leaves the individuals to learn from their own experiences and is a barrier to knowledge sharing for ID theft prevention in *Company Z.*

Table 5.9 Barriers to knowledge sharing for ID theft prevention in *Company Z*

S.No	Barrier in KS for ID theft prevention	Empirical Findings in *Company Z* (Barrier in KS for ID theft prevention)
1	Staff unwillingness	Yes
2	Lack of individual staff awareness	Yes
3	Insufficient learning opportunities	Yes
4	Distrust of other staff members	Yes
5	Fear of information leakage	Yes
6	Insufficient information sourcing opportunities and inefficient ICT infrastructure	Yes
7	Lack of leadership support	Yes
8	Weak knowledge sharing culture	Yes
9	No job rotation	Yes

Table 5.9 shows that staff unwillingness, lack of individual staff awareness, insufficient learning opportunities, distrust of other staff members, fear of information leakage, insufficient information sourcing opportunities and an inefficient ICT infrastructure, lack of leadership support, a weak knowledge sharing culture and no job rotation are barriers in the process of knowledge sharing for ID theft prevention in *Company Z.*

5.5. Chapter Summary

This chapter includes the empirical work of this study. It describes the data collected from three online retail companies, including semi-structured interviews, internal documents of the organisations and external documents. The total number of interviews was 34 from all three researched companies, and they were conducted with top management and lower level staff of various departments in the companies. The internal documents collected include policy documents, short memos and email conversations. The external documents include online retail industry reports published in various industry magazines, journal and conference proceedings, electronic and print media reports and reports published on the researched company websites.

From the investigation of the external documents, this study found that ID theft has become a major issue for online retail industry organisations in the UK. The organisations need to enhance the knowledge of individual staff members and teams for ID theft problems and its prevention, and the knowledge sharing processes for ID theft prevention in the organisations. On the other hand, the investigation of internal documents found that companies have the policies to secure the use of existing IT infrastructures, including the safe use of computers, company databases and communication networks. Various email and memo conversations showed that it is the responsibility of the information security related departments to protect the computerised systems.

This research found that individuals and teams have an awareness of those issues in the technical departments. On the other hand, staff from non-technical departments are not aware of ID theft issues.

The companies have provided learning opportunities at a fundamental level about the existing working environments and the computerised systems they use. At the moment, companies are not focusing on enhancing the knowledge of staff for ID theft prevention awareness. Staff from two of the three researched companies do not trust sharing such types of knowledge. Staff unwillingness, lack of individual staff awareness, insufficient learning opportunities, distrust of other staff members, fear of information leakage, insufficient information sourcing opportunities and inefficient ICT infrastructure, lack of leadership support, weak knowledge sharing culture and no job rotation are barriers to the process of knowledge sharing for ID theft prevention in online retail organisations.

Therefore, it is recommended that they implement an educational environment to enhance the knowledge of individual staff members and teams across the departments within their companies. Furthermore, companies should implement knowledge sharing processes for ID theft prevention.

CHAPTER 6 ANALYSIS AND DISCUSSIONS

6.1. Introduction

This chapter includes the analysis and discusses the data collected from the three online retail organisations and extends the knowledge sharing framework proposed by Salleh (2010) using the theory of KM.

There are various approaches for analysing qualitative data in the literature; the suggested analysis approaches are experimental and testing programmes, archival analysis, thematic analysis and content analysis. According to Pawson and Tilley (1997), and Joffe and Yardley (2004), these analytical methods answer the questions of what works, for whom, in what circumstances, and why. This study included a thematic analysis and was considered to fulfil the requirements of the current research established on a contextual reading of the knowledge sharing framework. The themes have been adopted from the guiding framework, and this study created new themes to fulfil the requirements of the investigation and provide a framework of knowledge sharing for ID theft prevention in an organisation. This chapter includes the analysis and discussion of the present study.

6.2. Cross-Case Comparison of Knowledge Enablers in the Processes of Knowledge Sharing for ID Theft Prevention

The enablers for knowledge sharing for ID theft prevention in the case organisations are discussed as follows.

6.2.1. KM Infrastructure

Technology is a key element in implementing a prosperous KM program and approach (Holsapple, 2013) as an efficient source for creating, storing and sharing information. ICT infrastructure refers to effective KM, based on persons sharing their knowledge through technological facilities that users throughout an organisation have access to (Holsapple, 2013; Martin, 2000). In any organisation, an updated ICT infrastructure helps the employees to generate, store and share knowledge between individuals, teams and departments (Syed-Ikhsan & Rowland, 2004). Investigation of the existing KM

infrastructure was prioritised to determine its limitations and provide proper recommendations for enhancing the knowledge sharing processes for ID theft prevention.

Company X has a strong infrastructure for ID theft prevention and various knowledge sharing tools are being used in the company, for example, Yammer, CIFAS, AQAFAX and KBA. The company has an e-learning system which provides information on training available to staff members. Employees also upload their activities on the e-learning system. A participant said:

> *"We have many systems that we use. I think for knowledge sharing the strongest that we use are the e-learning packages; if anything new comes out such as a new process, or new system, it is always done through e-learning."(Company X)*

Company policy documents are uploaded onto their website. Staff access these documents and sometimes they acquire information using their contacts in the company. This research found that basic skills are provided to the staff in *Company X,* for example, how to use and create Excel spreadsheets and pivot tables. Some of the employees are trained to analyse the data from their own experience about ID frauds and encountering those frauds. Even though employees have a lower level of skills, they are satisfied with the availability and usage of the existing resources, having the skills from their own experience to work in the company and use the existing systems.

Company Y also uses multiple tools to share knowledge among individuals and teams; these tools include Yammer, a centralised system they call 'Connect', SharePoint 2007, emails, an e-learning system, and LYNC. The company has uploaded their policy documents onto the website, which can be accessed using a user ID and a staff password. The participants are happy with the availability and usage of existing tools for knowledge sharing. However, knowledge sharing tools are not being used for knowledge sharing for ID theft prevention in the company. Participants of *Company Y* responded that:

> *"We have got many resources that we can share information with. I think probably out there; we are one of the best companies in it." (Company Y)*

> *"I am not sure what resource is used to prevent our identities being stolen." (Company Y)*

As with the other two researched companies, *Company Z* also uses various tools to share knowledge among the staff; these include Yammer, emails and an e-learning system.

They also have uploaded policy documents on the website of the company. Employees are satisfied with the availability of the knowledge sharing tools. A participant said:

"We have strong tools to share the knowledge of what we do." (Company Z)

The employees are also happy with the usage of the existing tools to share knowledge, but, as in *Company X* and *Company Y*, the existing tools are not used to share knowledge for ID theft prevention in *Company Z*. A respondent from *Company Z* said:

> *"I am really happy with IT systems available here; there are so many layers which help to avoid security issues. And we have a good knowledge sharing system too. But these systems are not used for ID theft prevention." (Company Z).*

Table 6.1 KM infrastructure for knowledge sharing for ID theft prevention in the organisation

Company	Strengths	Weaknesses	Recommendations
Company X	- Uses tools for ID theft prevention such as Yammer, CIFAS, AQAFAS and KBA. - Policy documents on the website of the company. - Has an e-learning system for updating the employees regarding available training.	- Does not provide knowledge for ID theft prevention. - Computerised infrastructure is not being used for knowledge sharing for ID theft prevention.	- A knowledge sharing system is required so that employees can share knowledge with each other and learn from others' experiences for ID theft prevention.
Company Y	- Uses SharePoint 2007, email, e-learning system, and LYNC. - Individuals are happy with availability and usage of knowledge sharing tools.	- Knowledge sharing tools are not being used to share the knowledge for ID theft prevention.	- It is recommended to use existing tools to share the knowledge for ID theft prevention. - Need to develop KM infrastructure to educate individuals and teams to share the knowledge for ID theft prevention.
Company Z	- Has knowledge sharing tools, such as Yammer, email and e-learning system. - Policy documents are uploaded on the website of the company. - Staff are satisfied with the availability of knowledge sharing tools. - Satisfactory KM infrastructure. - Has an e-learning system for updating the employees regarding available training.	- Existing tools are not being used to share the knowledge for ID theft prevention. - Individuals and teams are not getting advantage from existing tools to enhancing the knowledge for ID theft prevention.	- Knowledge sharing environment is needed. - The company should implement a knowledge sharing environment for ID theft prevention. - Staff from the non-technical departments require the skills of protection from ID theft issues.

Regarding the skills needed to share knowledge for ID theft prevention, participants from the call centre of the company need training to increase their awareness about ID theft issues and its prevention and how to share that knowledge with others in the company. Participants responded:

> *"I don't know about ID theft problems. I need help in it..." (Company Z)*
>
> *"I require awareness of ID theft issues and protection from it. If the company arrange some training and some seminars, I will be happy to attend." (Company Z)*

Table 6.1 summarises the KM infrastructure for knowledge sharing for ID theft prevention in online retail organisations, although participants are happy with the existing KM infrastructure. The resources required for them to perform their job roles are available, and they are satisfied with the usage of the existing resources. However, the current knowledge sharing tools are not being used to share their knowledge for ID theft prevention. Individuals and teams are not getting the advantage from the existing tools to enhance their understanding of ID theft prevention. A knowledge sharing system is required so that employees can share knowledge with each other and learn from others' experiences to prevent ID theft.

6.2.2. ICT Know-how and Training

ICT infrastructure plays a vital role in knowledge sharing among the individuals within and outside an organisation (Syed-Ikhsan & Rowland, 2004). It is essential to understand the ICT skills required to assess the ability of staff to use those skills to solve the complicated problems of information management, knowledge sharing and presentations (Cobo, 2013), which include learning and technological skills such as developing ideas, sharing information and fact finding (Cobo, 2013; Dede, 2010). Employees require particular practical skills ('know-how') to perform required tasks efficiently. These can be learned and developed through independent learning or detecting and emulating the skills of others, which are the approaches of a tacit knowledge sharing environment (Letmathe et al., 2012).

In this study, the aim of ICT know-how and training is to enhance the knowledge of individuals and teams to understand ID theft issues and its prevention.

All the three online retail companies researched provide very basic training to staff newly joining the company.

> *"When I first started, I was trained in every system we needed to use. I mean, we get like, someone will show us something new. It is not training. But someone will show us a new way of working and a new way of pulling information out, and we will just take them on board." (Company X)*

> *"When you join the company usually you have an induction to the building and the culture of the institution as a whole ... and there are also departmental inductions. And then within the job role then you got your specific training depending on your job role." (Company Y)*

> *"When I joined the company they provided training about the infrastructure, the way I work and how to deal with others in groups or the working environment."(Company Z)*

The companies are providing training to their staff for their job roles and the tools they use in the workplace of the company.

> *"We have had Excel training, spreadsheets, Access database training, things that we would need to produce our reports to the regional loss prevention managers."(Company X)*

> *"Guess that would be things like getting trained to know how to use the shared folders, to know how to use the shared software, and sometimes it is purchasing software as well that you need the training to be able to do."(Company Y)*

Of the researched companies, *Company X* provides technical training to the staff in the fraud prevention and information security departments, whereas staff from the information security and IT security departments of *Company Y* have technical know-how about ID theft issues and its prevention to some extent.

None of these companies provides training for sharing knowledge for ID theft prevention within their organisation.

One respondent from *Company X* said:

> *"...we are not doing anything like that; we do not need training for sharing the knowledge of id theft prevention." (Company X)*

Table 6.2 ICT know-how and training to share the knowledge for ID theft prevention in the organisation

Company	Strengths	Weaknesses	Recommendations
Company X	- Training for new employees. - Provides policy documents for working activities. - Arranges seminars to enhance the knowledge of the workers.	- Fundamental training to the employees, such as how to create spreadsheets in Excel and Access when joining the company. - A couple of departments provide training for ID theft and its prevention. - Individuals from non-technical departments are not provided with the know-how of ID theft issues and solutions.	- Needs to enable the employees of departments to have training for ID theft prevention. - Develop knowledge sharing system for ID theft prevention. - Develop the education of the workers in the process of knowledge sharing.
Company Y	- Department and company-wide inductions. Provides training according to the job role. - Scheduled training, refresher courses and seminars to enhance the knowledge of the workers. - Has policy documents for information protection procedures.	- Very basic training for the employees. - No training on ID theft prevention. - Lack of know-how for sharing knowledge for ID theft prevention. - To enhance the knowledge of staff for ID theft prevention.	- Individuals need the know-how about ID theft issues. - Staff in non-technical departments require learning opportunities to enhance the knowledge for ID theft prevention. - Develop knowledge sharing environment for ID theft prevention.
Company Z	- Departmental level and company-wide inductions. - Has scheduled training, refresher courses and seminars.	- Basic training at the level of know-how about IT infrastructure and usage of computers. - ID theft prevention training for staff from information security department only. - No policy of the knowledge sharing for ID theft prevention to other departments.	- Requires training on ID theft prevention and its knowledge sharing to employees of departments other than IT department. - Enhance the educational process the for knowledge sharing. - Requires the development of the knowledge sharing system for sharing the knowledge for ID theft prevention.

Investigating *Company Y*, the researcher found that, at the moment, the company is not focusing on enhancing the knowledge of individuals as well as teams about ID theft issues and its prevention. The literature shows that training is a learning opportunity to enhance technological skills for computer usage and knowledge sharing (Hortovanyi & Ferincz, 2015), and therefore, organisations provide various training opportunities to their employees to keep them up-to-date and enhance their knowledge (Dymock & McCarthy, 2006).

However, there is no training available to the staff that includes ID theft prevention awareness in all the researched companies, particularly for the staff members working in non-technical departments in these companies. A participant from *Company Y* responded that *"there is no mention of ID theft in training" (Company Y);* whereas staff from the technical department of *Company Z* have some sessions on ID theft prevention. A participant from the IT department responded:

> *"We have training for how to secure the systems and I had a session for ID theft prevention during the IT security training."(Company Y)*

Again, *Company Z* is not focusing on educating the staff to share their knowledge for ID theft prevention.

A learning environment leads the organisations to the peak of success; it defines procedures leading to accumulative capabilities and skills through routine work (Mohammad Hossein & Nadalipour, 2016). An advanced learning environment enables the workers to enhance their expertise to deal with complicated problems, and learning opportunities enhance progress by removing previous mistakes and weaknesses (Harteis et al*.,* 2008). Organisations provide various training opportunities for their employees to keep them up-to-date and to enhance innovative techniques to improve performance (Ibid*.)*. Table 6.2 describes the ICT know-how and training to share knowledge for ID theft prevention in the organisation.

Training and other learning opportunities such as street shows, seminars and conferences can play a major role in increasing the knowledge of staff regarding ID theft prevention. Participants from all three companies require training and other learning opportunities to enhance their knowledge for ID theft prevention. Table 6.2 shows that currently, the researched companies focus on ID theft prevention at customer level; they do not concentrate on the development of knowledge sharing processes for ID theft prevention in their companies. Therefore, it is recommended that they build a culture of knowledge sharing for ID theft prevention within the organisations and educate the individuals as well as the teams.

6.2.3. Job Rotation

Knowledge shared among individuals is concerned with establishing communication among workers inside the organisation. The most significant issue of knowledge sharing is the trust within the organisation (Bălău & Utz, 2016; Hashim & Tan, 2015). For example, how willing are people to share what they know? Answering these questions leads us to activities based on trust building, team creation, job rotation and so forth (Sveiby, 2001).

Regarding the investigation of the process for job rotation in *Company X*, the researcher found that here is no job rotation there. A participant responded:

> *"There is not any job rotation." (Company X)*

Another participant said:

> *"We do not do any job rotation really with anybody else." (Company X)*

Due to not having a policy of job rotation in *Company X,* individuals are not getting any advantage of learning from others' experiences, and staff have no chance to learn from the new environment of other departments of the company. They are learning from their own experiences.

On the other hand, *Company Y* has a strong process of job rotation - all participants responded with *"Yes"* to the enquiry about job rotation and all staff members pass through the process of job rotation. New employees joining the company are provided with training and move into different departments during their probationary period.

A participant from *Company Y* responded that:

> *"When the graduate starts right after university to join us, we have got very structured training programmes for them. So they take six months role in different departments of their choice." (Company Y)*
>
> *"So once your secondment is finished, let's say you worked there for six months, then ... you can go back to your own job. So you can learn something new ... if you do not find the permanent position in your new team, you can go back." (Company Y)*

Individuals and teams are getting the advantage of job rotation in the company; they learn from a new environment and the experiences of others working in a different team. An interviewee responded:

"…because they do something else. And it expands the experience. And it means that you know, we do not have a single point of failure because somebody else can do his or her job too." (Company Y)

Another participant responded:

"Yeah, because let's say if someone comes into my team then the person who was working on the team would be training the new person now." (Company Y)

This study found a strong culture of job rotation in *Company Y*. The literature shows that job rotation plays a vital role in enhancing the knowledge of individual employees and teams within and outside any department in an organisation (Aga et al*.,* 2016; Huang & Pan, 2014; Ortega, 2001). Therefore, it is useful in enhancing the knowledge sharing processes for ID theft prevention in the organisation, and individual staff members and teams can get the advantage.

While researching *Company Z*, the researcher found that there is no job rotation in the company; some participants are not even aware of it. Participants responded that:

"I do not know about the job rotation."(Company Z)

"We do not have any process of job rotation in the company."(Company Z)

Staff are learning from their own experiences, and they think they do not need help from outside the department to learn something. A respondent said:

"I gain knowledge from things I do here, I do not need to go anywhere and ask how to do my work. That is why my job is not ever rotated."(Company Z)

A participant from management level said:

"Our staff are very experienced in their work and do not need to go to other departments to learn about their environment."(Company Z)

By investigating all three companies, the researcher found that *Company Y* has a system of job rotation where individuals and teams/groups are getting the advantage of experiencing a new environment; they learn from the experiences of others working in different teams and groups from other departments.

On the other hand, *Company X* and *Company Z* do not have a culture of job rotation (see Table 6.3), and staff learn from their own experience. As discussed earlier, job rotation plays a vital role in enhancing the knowledge of individuals and teams working in

different departments (Kane et al., 2005). Therefore, it is recommended that all the researched companies should implement a job rotation process to enhance the knowledge of staff members for ID theft prevention in the organisation.

Table 6.3 Job Rotation to increase the knowledge of individuals and groups for ID theft prevention

Company	Strengths	Weaknesses	Recommendations
Company X	- No job rotation.	- No job rotation. - Individuals from departments and teams are not benefiting from others' experience.	- Job rotation process to enhance the knowledge sharing for ID prevention.
Company Y	- The company has a job rotation process. All newcomers pass through different departments. - Individuals move from one department to another of their choice. They enhance their knowledge by working with others in different departments. - Teams get the advantage of staff whose job is being rotated (a newcomer in the department).	- Jobs are not rotated to enhance the knowledge of others for ID theft prevention in the company.	- Job rotation to enhance the knowledge sharing process for ID prevention.
Company Z	- No job rotation.	- There is no job rotation. Staff are not getting the advantage of others' knowledge and experiences.	- To implement the process of job rotation so that individuals and teams/groups can learn from the person coming into the new environment and team/department.

Job rotation can play an important role in increasing the knowledge of staff to prevent ID theft in the company, and it can be useful to provide awareness to the individuals as well as teams regarding ID theft issues and how to deal with these matters. Table 6.3 shows that *Company X* and *Company Z* do not undertake job rotation at all and *Company Y* has a job rotation process, but this research did not find any job rotation to enhance the knowledge of staff to prevent ID theft. Therefore, job rotation is recommended to increase the knowledge of others.

6.2.4. Feedback on Performance Evaluation

Feedback is vital for the evaluation and monitoring of the activities of employees, and current developments in electronic technology have advanced the nature of monitoring performance (Alder & Ambrose, 2005). Feedback can be given for various purposes, which include bringing the outcomes of activities or processes into focus; providing information when workers move away from primary goals; helping to fix new goals or adjusting the current goals; and guidance to perform activities. It also promotes critical reflection and brings about new approaches (Gabelica et al., 2012).

The researcher found an evaluation process in all three researched companies. Managers arrange meetings with staff members every month, discuss progress and then provide feedback to them in one-to-one meetings. A participant from *Company X* responded that:

> *"We have a monthly accreditation where the manager would listen to calls so they should see that we had not done something correctly or we could have handled that little bit better. Feedback would be given in our one-to-one meeting." (Company X)*

Another participant said:

> *"Once a month with our manager and she tells us how we are doing." (Company X)*

Company Z has a policy of checking the performance of their employees where managers see staff on a monthly basis and discuss the progress in their work.

An interviewee from *Company Z* said:

> *"We meet every month; my manager asks me about the job I did during the month. He notes in the diary and sends me an email with feedback on my performance." (Company Z).*

Company Y is quite right in the evaluation of employees and provides feedback to them. The company has an evaluation policy at both departmental and organisational levels. Managers meet one-to-one with the staff monthly at the departmental level. In those meetings, the manager checks out the performance of staff and then provides them with feedback. The feedback is based on the work done, the tasks accomplished and the behaviour of the staff with others. At the organisational level, the company evaluates the performance of staff twice a year. Every employee needs to fill in a pro forma they call

an appraisal.

A participant of *Company Y* replied:

> "*So there is a, you know, target setting and performance setting in place for employees, so there is, you know, sort of 6 months and 12 months sort of reviews of the job."(Company Y)*

Staff from *Company Y* and *Company Z* have evaluation reviews at the end of the year. Participants responded that:

> *"Employees have to write it annually; they call it end-of-year or half-year performance review." (Company Y)*

> *"I fill online pro forma by the end of the year." (Company Z)*

Company X, however, has the policy of evaluation and providing feedback at an organisational level twice a year. A participant from *Company X* responded that:

> *"We have a performance review every six months." (Company X).*

For investigating any existing tools used for evaluating the knowledge of staff, the researcher found that from all these researched companies, *Company X* provides a tool they call the 'e-learning system'. The e-learning system includes various modules and staff are required to study these modules and are examined electronically on that system. Individuals need to get a 100% score otherwise they are bound to undertake training for the modules they fail.

A participant responded:

> *"…e-learning section of the internet and they have done that mini course or the events of those series of 10, 15 questions. So they should know, or they should have a grounding of what's expected of them as regards ID theft." (Company X)*

There is no process for evaluating the performance of employees regarding the knowledge sharing for ID theft prevention in any of the researched companies.

Interviewees responded in words:

> *"We are not evaluating the performance for ID theft prevention knowledge sharing. And there is no feedback for that. Or I can say our evaluation is not about knowledge sharing to prevent ID theft." (Company X)*

> *"… ID theft prevention is not in that criteria. It is the evaluation of our job we do*

here, not the knowledge sharing for it." (Company Y)

"No ID theft is mentioned in our performance review." (Company Z)

According to Shapero (1985), performance evaluation helps with training, continuous learning, boosting robust performance, and consolidating poor performance. Therefore, feedback on a performance evaluation is a significant motivator for individuals (Gould-Williams, J. S. 2016). It is a means for reception of information needed to improve greater know-how and improvement in their profession (Taylor et al., 2001). Table 6.4 summarises the feedback on performance evaluation for sharing the knowledge for ID theft prevention.

Table 6.4 Summary of feedback on performance evaluation for knowledge sharing for ID theft prevention

Company	Strengths	Weaknesses	Recommendations
Company X	- The performance of the employees is evaluated for routine work and tasks given to staff. - Have monthly meetings for evaluating the performance. - Managers provide feedback to staff in one-to-one meetings. - Evaluate the performance twice a year.	- Not evaluating the performance of the knowledge sharing of employees for ID theft prevention.	- Need to evaluate the knowledge level of staff for ID theft prevention. - Need to provide feedback for awareness for ID theft issues and its prevention.
Company Y	- Performance at departmental and organisational level. - Appraisals twice a year. - The Strong impact of performance evaluation of employees. - Monthly evaluation meetings with departmental managers. - The performance of individuals is being evaluated for working activities, and feedback is given based on results.	- Performance is not evaluated for knowledge sharing for ID theft prevention. - There is no feedback for the knowledge sharing for ID theft prevention.	- Needs to develop the culture of performance evaluation for the knowledge sharing for ID theft prevention.
Company Z	- The company provides feedback to the staff on a monthly basis. - All staff go through performance evaluation every month.	- No performance evaluation process for sharing the knowledge for ID theft prevention. - No feedback for ID theft prevention knowledge.	- Staff evaluation is required for the knowledge level of staff for ID theft prevention awareness. - Feedback may be provided to staff for ID theft prevention awareness.

Evaluation feedback can play an important role in enhancing the knowledge of individuals in the organisation for preventing ID theft and share its knowledge. Table 6.4 shows that feedback on performance evaluation is not being provided for ID theft prevention awareness. Therefore, it is recommended that companies implement a culture of performance evaluation for sharing the knowledge for ID theft prevention within their organisation.

6.2.5. Information Sourcing Opportunities

Brown and Starkey (1994) presented the concept of information awareness to be generated in an organisation, which relates to the attitude of the organisation to considering information as a resource and the consequential procedures of making organisational learning or knowledge available by expediting knowledge sharing among the workforce. It is important for organisations to considering information as a resource in the organisation (Holsapple, 2013). Consequential procedures of making organisational learning or knowledge available by expediting knowledge sharing among the skilled workforce are inevitable (Khan et al., 2016; Bhatt et al., 2010). Therefore, information sourcing opportunities or ease of gaining information is vital for the knowledge sharing for ID theft prevention among individuals and teams. Consistent contact or a communication network to proficient information, or a degree of technical and professional knowledge, is easily obtainable and available from individual staff members who are examples of information sourcing opportunities.

While investigating *Company X*, the researcher found that the company has a policy of ID theft prevention as they use multiple resources to share information, including the policy documents of the company which contain information on how to protect, how to secure the computers, and how to use the existing resources in the company.

For communication, individuals and teams use emails, and they have an internal networking system in the company they call ‘blackboard’, which is used to update the staff regarding upcoming events, availability of training and any security issues the company have. They also use a corporate social network they call ‘Yammer’, through which individuals and groups share knowledge with each other. A participant from *Company X* responded that:

"We use email, we have got internal network messaging which is YAMMER. We have got policy documents from theft, fraud, to money laundering. We have got all them type of documents all the way through. And obviously, we have all got these iPhones and what have you."(Company X)

Company Y is right at the availability of information sourcing opportunities, as they have various information sourcing opportunities provided to the staff, such as the staff has access to the e-learning system which is called 'e-portal' and they use a messaging service called 'Yammer'. The company website contains numerous documents which could be useful to the staff in their day-to-day jobs, and also includes a schedule of work activities. Staff access SharePoint and use email, company seminars and street shows. Managers update their employees using PowerPoint presentations. There is a library in the company building which has a huge amount of literature available for staff to enhance their knowledge. A participant responded:

"…Emails, internal network messaging system and policy documents. All of these are shared with the employees. Most of the communication is done on email sharing. We have got our own internet site like a website but only for us to view internally. A lot of information is sent out on that news bulletin. So this is available from that perspective."(Company Y)

Company Z is also as good as *Company Y,* as information sourcing opportunities are available to the staff at *Company Z* including Yammer, email and policy documents. Information is shared in the company using email and policy documents are available on the website of the company including information about how to work in the company, and how to use the existing facilities including IT equipment or other resources. A respondent said:

"My manager send me email what things to do and when to do…" (Company Z)

During investigating all three companies, the researcher found that knowledge for ID theft prevention is being shared at the departmental level in *Company X;* they use their available resources for it, whereas in both *Company Y* and *Company Z*, the available information sourcing opportunities are not being used to share knowledge for ID theft prevention.

Participants responded:

"…the way we work today is we would email, we have companywide email that would go out to remind people that it was time for them to re-intake the security awareness education that would be this…"(Company X)

"It is nothing like there's a company-wide policy on ID theft prevention."(Company Y)

"I do not know how to share ID theft prevention knowledge."(Company Z)

While investigating the requirement for further information sourcing opportunities, the researcher found that individuals need awareness of ID theft issues and how to protect personal and organisational information from ID thieves.

Table 6.5 Summary table for information sourcing opportunities

Company	Strengths	Weaknesses	Recommendations
Company X	- The company has a policy of ID theft prevention. - Uses an internal network messaging system to broadcast information within the company. Emails update employees on ID theft issues.	Individuals are not sharing their expertise and methods regarding ID theft prevention.	- More resources could be provided to the staff for the knowledge sharing for ID theft prevention. E-learning system could be enhanced as a source of the knowledge sharing for ID theft prevention and increase skill levels.
Company Y	- Have internal network messaging system to share information called 'Yammer'. - Use Microsoft SharePoint 2007. - Implement a centralised system called Connect. - Use emails to update staff. - E-learning system called e-portal on the website of the company. - PowerPoint presentations to the staff. - The company has a library with a huge range of literature.	- These sources are not being used for sharing the knowledge for ID theft prevention. - Do not have a policy of ID theft prevention. - No use of existing opportunities for sharing the knowledge of ID theft prevention.	- Need to focus on the usage of existing information sourcing opportunities for the knowledge sharing for ID theft prevention. - Need to set a policy for the use of sources to enhance the knowledge of individuals for ID theft prevention. - Enable teams to use information opportunities for ID theft prevention awareness. - More resources could be provided to the staff for effective knowledge sharing for ID theft prevention.
Company Z	- Uses an internal messaging system called 'Yammer'. - Provides policy documents to the staff. - Email communications.	- Information sourcing opportunities are not being used for the knowledge sharing for ID theft prevention in the company.	- It is recommended to facilitate the individuals as well as the teams with opportunities for sharing the knowledge for ID theft prevention.

All three companies have provided different information sourcing opportunities to work in the company and share required knowledge with others within the working environment (see Table 6.5).

Existing literature includes the importance of information sourcing opportunities in organisations (Holsapple, 2013); these opportunities are useful in the process of knowledge sharing (Khan et al., 2016; Bhatt et al., 2010). However, existing information sourcing opportunities are not being used for sharing the knowledge for ID theft prevention in all the researched companies. Online retailers are not concentrating on raising the awareness of their staff for ID theft issues and its prevention (see Table 6.5). Existing information sources can be used for sharing knowledge for ID theft prevention inside the companies where individuals, as well as teams and departments, can make use of these opportunities to enhance their knowledge regarding ID theft identification and its prevention.

6.2.6. Leadership Support

Leadership has a major role in managing the knowledge sharing processes in any organisation (Muethel & Hoegl, 2016; Bass & Stogdill, 1990). Leadership is accountable for practising strategic planning for the best use of means and promoting a learning culture and knowledge sharing. The leadership are required to bring about an open culture and to build an environment for knowledge sharing. Furthermore, top management should provide support to enable the value of knowledge sharing support to those requesting knowledge sharing approaches. Importantly, senior executives and the top management should reveal the distribution of their knowledge and use the knowledge of others in taking their actions, and provide rewards to those who share their knowledge (Aga et al., 2016; Barnes, 2001).

During investigating all three companies, the researcher found strong communication process from top management to lower level management (top-down communication).

Management uses different ways to share information with staff, which includes one-to-one meetings, emails, seminars, and street shows and conferences.

A participant from *Company X* responded:

> *"We have managers' meetings every single month; we have a buzz of managers' emails."(Company X)*

"There is a cascade of information being done via email, and so there are regular email briefings that come out as well as obviously the emails, cascade emails as well."(Company Y)

In *Company Z* the management arranges information sessions and discuss the activities they do in the organisation. A respondent of *Company Z* said:

"We have a meeting on a monthly basis. Sometimes our directors brief us in general discussions." (Company Z)

Table 6.6 Leadership support to enhance the knowledge sharing processes for ID theft prevention

Company	Strengths	Weaknesses	Recommendations
Company X	- Leadership is supportive of the workers and staff happy with the facilities provided.	- More workforce is needed to prevent ID theft.	- Leadership could facilitate the staff to educate them in how to share the knowledge for ID theft prevention. - Technical education and training are needed for a better environment.
Company Y	- Share information using email. - Leave general messages on Yammer. - Arrange meetings with subordinates. - Arrange seminars for staff awareness. - Supportive leadership. - Staff are happy with management.	- Leadership is not motivating staff to enhance their knowledge for ID theft prevention. - ID theft prevention knowledge sharing is not in focus of management of the company.	- A communication process for knowledge sharing for ID theft prevention. - Provide a learning environment for enhancing knowledge of ID theft issues and its prevention. - Facilitate the workforce with education about an enabling knowledge sharing process in non-technical departments.
Company Z	- Helpful and supportive leadership. - Fulfil all requirements. - Share knowledge via meetings, emails and phone calls.	- Not focused on increasing the knowledge of staff to prevent ID theft and share its knowledge.	- Leadership required to implement a knowledge sharing environment. - Develop educational environment to increase the knowledge of staff for ID theft prevention.

Managers in *Company X* sometimes walk down to the desks of the staff and discuss what they need.

"Our department managers want to relay any information regarding that buzz of email; sometimes she poses in our office and we will have a quick buzz session

meeting, or she can come to your desk to speak to you. There are quite a few different ways." (Company X).

Table 6.6 describes leadership support required for knowledge sharing for ID theft prevention in the online retail organisations; it also summarises the discussions about the knowledge sharing processes of leadership to the staff.

The literature review describes how management should provide support to enable the value of knowledge sharing support to those requesting knowledge sharing approaches (Mittal & Rajib, 2015). Table 6.6 shows that the leadership of all three companies is very supportive and helpful and the staff are happy with their management. However, the leadership in all three of the researched companies do not support the process of knowledge sharing for preventing ID theft in the organisations. There is a need for an enhanced environment for knowledge sharing for ID theft prevention. Leadership support is required to develop an educational environment for enhancing the knowledge of ID theft prevention and sharing its knowledge within the organisations so that individuals and teams from different departments can get the advantage of knowledge sharing for ID theft prevention in their companies.

6.2.7. Knowledge Sharing Culture

Organisational culture refers to the shared values, beliefs and performances of persons within an organisation (McDermott & O'Dell, 2001). Knowledge sharing culture is the main element considered for knowledge sharing among individuals and teams within the organisation; it is the most important factor that needs to be understood in advance before employing any new strategies in the organisation (Syed-Ikhsan & Rowland, 2004).

A knowledge sharing culture is considered to be a significant aspect since it controls the effects of other related variables such as the existing technology and management techniques on the accomplishment of KM. According to Stoddart (2001), knowledge sharing can only work if the culture of the organisation supports it, and if the changes required are developed according to the culture of the organisation.

During investigating *Company X* for the knowledge sharing culture for ID theft prevention in the company, the researcher found that employees trust other workers concerning knowledge sharing for ID theft prevention within their department, but they do not trust the people outside their department, such as the staff from other departments.

Currently, knowledge is being shared only within departments of the company. A participant said:

> *"I would not ever go outside the fraud department for any knowledge; there is no reason I will need anything from outside the fraud department; all the information is here, you just need to find the right person." (Company X)*

Another participant responded:

> *"If it is in a different department we would double check that. In confirming from ourselves that it is fraud before taking it that it is the fraud that was within the department, then yeah, we trust them, we follow on their action." (Company X)*

Trust of others is one of the key elements in the process of knowledge sharing (Bălău & Utz, 2016; Hashim & Tan, 2015). However, employees are not confident enough to share their knowledge with the staff of other departments to prevent ID theft, due to a lack of trust. Therefore, individuals and teams are only getting the advantage of the expertise within their department. *Company X* needs to develop a system to educate the staff from different departments and raise awareness of ID theft and its prevention. They need to increase the level of trust within the organisation.

On the other hand, *Company Y* has a strong culture of knowledge sharing. Individuals and teams are sharing knowledge with each other both within and outside their departments.

A participant responded that:

> *"…there are no particular restrictions on sharing knowledge with other departments. So we are quite open regarding sharing knowledge and obtaining knowledge from other departments."(Company Y)*

Knowledge sharing culture contains the trust of others, communication with others and the behaviour of the existing information system. Staff will work efficiently if they have the trust of others working with them (Safa et al., 2016; Roth & Broad, 2008; Hsu et al., 2007; Bos et al., 2002; Ridings et al., 2002); it is the backbone of the knowledge sharing process in any organisation. During investigating the communication of information with others, the researcher found that the staff are satisfied with the process of communication among individuals and teams with and outside their departments in the company. The participants were happy with the existing information systems of the company.

The investigator found that there is no culture of knowledge sharing for ID theft prevention. The participants require a cultural change from top to bottom in the company concerning sharing the knowledge of ID theft. They need training, education and awareness regarding ID theft issues and solutions to protect the organisational and personal information from fraudsters, requiring a computerised environment that could be used for sharing the knowledge for ID theft prevention.

Company Z has a sound knowledge sharing culture at departmental level where staff trust each other within their departments. A participant said:

> *"I trust my friends who work with me. We work together and support each other to maintain the system and provide IT facilities in the company." (Company Z)*

Another respondent said:

> *"I trust them because they work with me and we need to share our work information. We are the security department; we must help each other and secure the systems here." (Company Z)*

Staff do not trust those with whom they do not work, and they are reluctant to share knowledge with others outside their department. Due to that, individuals and teams are not getting the advantage of knowledge sharing outside their department. When asked about sharing the knowledge for ID theft prevention, a participant responded:

> *"I do share ID theft knowledge with my friends who work with me, but I do not share such type of information with the people I am not working with."(Company Z)*

Table 6.7 describes the knowledge sharing culture in the online retail organisations for ID theft prevention. Staff get the advantage of sharing their knowledge for ID theft prevention in information technology and information security departments. Trust and sincerity could support dynamic knowledge sharing performances through successful communication by providing a mandate to the members of the organisations to share the knowledge that they possess (Pervaiz et al*.,* 2016). Staff from non-technical departments need to enhance their trust level, and they need to be educated regarding improving their knowledge of ID theft prevention.

Table 6.7 Knowledge sharing culture of ID theft prevention

Company	Strengths	Weaknesses	Recommendations
Company X	- Different teams get the advantage of knowledge sharing. - Staff are trusted. - Employees are happy with existing IS.	- Personnel from other departments do not benefit from the knowledge. - Lower confidence in staff from other departments.	- Need to increase the trust level. - Need to educate the workers from other departments to share knowledge.
Company Y	- Different teams get the advantage of knowledge sharing. - Staff are trusted. - There is a culture of knowledge sharing outside the department in the company. - Employees are happy with existing information system.	- There is no culture of the knowledge sharing ID theft prevention. - Individuals have no knowledge of how to share knowledge for ID theft prevention.	- Needs to develop a knowledge sharing culture for preventing ID theft.
Company Z	- The company has knowledge sharing culture at the department level. - Staff are trusted at the department level in the company. - The knowledge is being shared for ID theft prevention within IT and information security departments.	- Knowledge is not being shared outside the department in the company. - Staff from other departments are not trusted. - No culture of ID theft prevention knowledge sharing. - Only two departments have a culture of the knowledge sharing for ID theft prevention.	- Employees from non-technical departments need to enhance their understanding of ID theft prevention. - The enhanced trust level is needed in non-technical departments.

Table 6.8 summarises the knowledge enablers required to share the knowledge for ID theft prevention in the organisation, describing the literature findings for the need of a knowledge enablers in the processes of knowledge sharing for ID theft prevention in the organisations. It also includes the availability/use of knowledge enablers to share the knowledge for ID theft prevention in the researched companies and the recommendations of this study.

6.3. Summary of Knowledge Sharing Enablers Required for Sharing Knowledge for ID Theft Prevention in Online Retail Organisations

The present study considered the knowledge enablers needed in the process of knowledge sharing for ID theft prevention in online retail organisations, which include: a KM infrastructure, ICT know-how and training, job rotation, feedback on performance evaluation, information sourcing opportunities, leadership support and knowledge sharing culture. Table 6.8 shows the literature findings for the need for the knowledge enablers required for sharing knowledge in any organisation and the findings from all three researched companies for the availability and use of these enablers. It also includes the recommendations of the present study.

The current study found the existing KM infrastructure is not being used for sharing the knowledge for ID theft prevention. The knowledge sharing tools are not being used to share the knowledge for ID theft prevention. Individuals and teams are not getting the advantage of the existing KM infrastructure for enhancing their knowledge for ID theft prevention. Therefore, the organisations should design and implement an effective KM infrastructure for the knowledge sharing for ID theft prevention (see Table 6.8). The literature gives importance to learning opportunities to enhance the knowledge of individual staff members and teams working in the organisation.

This study found all three researched companies provide very basic training to staff newly joining the company. The companies provide training for the staff for their job role and the tools they use for work. However, there is no training available to the staff that includes ID theft prevention awareness in all the researched companies, particularly for the staff members working in non-technical departments in these companies. Therefore, the organisations should design a comprehensive ICT know-how and training programme to educate the staff to share the knowledge ID theft prevention.

The literature shows that job rotation enables individuals to learn from various departments, decreases employee exhaustion caused by tedious or boring job tasks, and increases both an individual's confidence and their satisfaction in the job (Kampkötter et al., 2016; Eriksson & Ortega, 2006; Huang et al., 2005;Triggs & King, 2000). It plays a major role in enhancing the knowledge of employees to prevent ID theft and share their knowledge for ID theft prevention (Kane et al*.,* 2005). The present study found that there is no job rotation process in *Company X* or *Company Z*. *Company Y* has a job rotation process, but it is not being used to enhance the knowledge of individual staff members to

share their knowledge for ID theft prevention in the company (see Table 6.8). Therefore, online retail organisations should enable a job rotation process to enhance the knowledge of individuals and teams.

Table 6.8 Summary of knowledge sharing enablers required for sharing knowledge for ID theft prevention in online retail organisations

KS Enablers for Knowledge Sharing Processes for ID Theft Prevention	**Literature Findings (need for KS Enabler availability)**	**Use of KS Enablers for Knowledge Processes for ID Theft Prevention**			**Recommendations of This Study**
		Company X	***Company Y***	***Company Z***	
KM Infrastructure	Yes	No	No	No	The organisations should design and implement an effective KM infrastructure for knowledge sharing for ID theft prevention.
ICT Know-How and Training	Yes	No	No	No	The organisations should design a comprehensive ICT know-how and training programme to educate the staff to share the knowledge for ID theft prevention.
Job Rotation	Yes	No	No	No	The organisations need to enable a job rotation process to enhance the knowledge of individuals and teams.
Feedback on Performance Evaluation	Yes	No	No	No	The organisations need to implement an employee evaluation process and provide feedback to them regarding knowledge sharing for ID theft prevention.
Information Sourcing Opportunities	Yes	No	No	No	The online retail organisations need to enhance information sourcing opportunities and use them for knowledge sharing for ID theft prevention in the organisations.
Leadership Support	Yes	No	No	No	Support of leadership is required for the individual staff members and teams to share their knowledge for ID theft prevention in the organisations.
Knowledge Sharing Culture	Yes	Department level	No	Department level	The organisations should develop a culture of knowledge sharing for ID theft prevention on organisational. The trust of other staff members working in non-technical departments should be increased for knowledge sharing for ID theft prevention in the organisations.

Current developments in electronic technology are advancing the nature of monitoring the performance of employees (Alder & Ambrose, 2005). Feedback is vital for the evaluation and monitoring of activities of employees. It can be given for various purposes which include bringing the outcomes of activities or processes into focus; providing

information when workers move away from primary goals; helping to fix new goals or adjusting the current goals; and guidance to perform the activities. It also promotes critical reflection and brings about new approaches (Gabelica et al., 2012).

All of these researched companies evaluate the performance of staff. Managers hold monthly meetings with employees and provide them with feedback on their performance. However, the present study did not find the process of feedback on performance evaluation for knowledge sharing for ID theft prevention in any of these organisations. The organisations need to implement an employee evaluation process and provide feedback to them for sharing the knowledge for ID theft prevention.

It is important for organisations to consider information as a resource in their organisation (Holsapple, 2013). Substantial procedures for making organisational learning or knowledge available by expediting knowledge sharing among the skilled workforce are essential (Khan et al., 2016; Bhatt et al., 2010). Information sourcing opportunities or ease of gaining information is vital to the knowledge sharing for ID theft prevention among individual staff members and teams. Consistent contact or communication networks with proficient information or a degree of technical and professional knowledge that is easily obtainable and available to individuals are specimens of information sourcing opportunities.

All three companies provide different information sourcing opportunities in the company and share required knowledge with others within the working environment. However, the online retailers are not concentrating on the awareness of ID theft issues and its prevention to their staff. Existing information sources can be used for sharing the knowledge for ID theft prevention inside the companies. Individuals, as well as teams and departments, can avail themselves of these opportunities to enhance their knowledge of ID theft identification and its prevention. Therefore, the online retail organisations need to enhance information sourcing opportunities and use them for knowledge sharing for ID theft prevention in organisations.

The literature shows that leadership plays an important role in managing knowledge sharing process in any organisation (Muethel & Hoegl, 2016; Bass & Stogdill, 1990). It is accountable for practising strategic planning for best use of means and promoting a learning culture and knowledge sharing (Boerner et al., 2007). The present study found a supportive leadership in the researched companies, where staff are happy with their management. However, there is the need for an enhanced environment for knowledge

sharing for ID theft prevention. Leadership support is required to develop an educational environment for enhancing the knowledge for ID theft prevention and sharing its knowledge within the organisations. Their support is needed by the individual staff members and teams to share knowledge for ID theft prevention in the organisations.

According to Stoddart (2001), knowledge sharing can work if the culture of the organisation supports it, and changes need to be developed according to the culture of the organisation, as having a weak culture of knowledge sharing causes hurdles to the knowledge sharing process. Therefore, it needs to be managed for an effective knowledge sharing process in the organisations. This study found that *Company X* and *Company Z* have a knowledge sharing culture at the departmental level, and staff are trusted at the departmental level. However, individual staff members and teams are not ready to share their knowledge with others outside their department within their company. While talking about *Company Y,* this study found a good culture of knowledge sharing where staff are ready to share their knowledge with anybody working in the company. However, there is no culture of knowledge sharing for ID theft prevention in *Company Y,* and therefore it is recommended that the organisations develop a culture of knowledge sharing for ID theft prevention between different departments in the organisations. The trust of other staff members working in non-technical departments should be increased for knowledge sharing for ID theft prevention in the organisations.

6.4. Existing Barriers in Knowledge Sharing for ID Theft Prevention in Online Retail Organisations

The literature shows that managing individual learning to assure effective knowledge sharing in organisations is hard to handle (MacNeil, 2003), where an organisation is following a management strategy aimed to retain and develop highly talented and motivated staff who are known to be vital for current and future accomplishments. That organisation tries to use the skills and knowledge of their employees to create intangible assets which cannot be replaced by their comparatives (Boxall, 1996) and hence the process of learning in organisations, which is required for the formation and sharing of knowledge, must produce an essential capability signifying a form of valued, knowledgeable human resource for the organisations (Valentine St Leon, 2002).

However, there can be various barriers to knowledge sharing for ID theft prevention in online retail organisations which impact on the knowledge sharing processes between individual employees and teams within or outside departments in online retail organisations. The present study identified the following barriers in knowledge sharing for ID theft prevention in online retail organisations.

6.4.1 Staff Unwillingness

Staff willingness plays a key role in the process of knowledge sharing. The literature describes that measures taken for knowledge sharing highly depend on the willingness of the employees working in the organisation (Hislop, 2002). The approach of workers to share their knowledge can be motivated by their awareness of their responsive connectivity with working in the organisation (Scott Holste & Fields, 2010; Hislop, 2002). These perceptions affect the willingness of staff members to commit to the organisation and employees with satisfaction in their jobs and the commitment to their organisations are willing to share their knowledge. They believe that the advantages of the organisation are to their benefit. Table 2.11 shows that individual staff members' willingness is necessary for an effective knowledge sharing process for ID theft prevention in the organisation. Individual staff unwillingness is a barrier in the knowledge sharing process for ID theft prevention in the organisation.

From the investigation in *Company X,* the researcher found that the employees are willing for knowledge sharing for ID theft prevention in their department within the company.

A participant from *Company X* said:

> *"Only I can share any knowledge with the people I work with. I do not discuss with the people who work in other areas of the business." (Company X)*

Staff are not ready to share their information with employees working in non-technical departments in *Company X*.

On the other hand, staff members are ready to share their knowledge with others within and outside their departments in *Company Y, as* an interviewee responded:

> *"I am happy to share the knowledge with other members of the company. It will be helpful to increase knowledge of others and mine too." (Company Y)*

Another participant of *Company Y* said:

> *"I do not know much about ID theft, but if anyone tells me about it, I will get it." (Company Y)*

The researcher found that employees are happy and willing to share knowledge with other staff members within and outside their department in *Company Y*. Therefore, staff unwillingness to share the knowledge for ID theft prevention is not a barrier in *Company Y*.

Workers in *Company Z* are willing to share their knowledge in their department. A respondent in *Company Z* stated:

> *"I am happy to discuss with my friends who work here, but I will not share any knowledge outside this department." (Company Z)*

However, individual staff members are not willing to share the knowledge for ID theft prevention with others working outside their department in the company. A participant from the information security department responded:

> *"I do not share it with others, and I am not ready to share the knowledge with them. It is not the policy of the company." (Company Z)*

The management of the company is not focusing on the willingness of individual staff members to share their knowledge for ID theft prevention in *Company X* and *Company Z*.

While enquiring about the reason for not being willing to share knowledge with others outside the department, the researcher found that there is no environment of knowledge sharing for ID theft prevention outside the department in these companies. There are no rewards or incentives for sharing knowledge with others, and therefore, individuals are not willing to share knowledge with others. Another reason for staff unwillingness is that they are bound by the rules and regulations. They cannot share knowledge with anybody with whom they do not work unless anybody needs help to solve issues. Therefore, staff unwillingness is a barrier to knowledge sharing for ID theft prevention in *Company X* and *Company Z*.

This research study agrees with the literature findings (see Table 2.11) for the need for an individual staff member's willingness to share knowledge. Therefore, staff unwillingness

is a barrier to knowledge sharing for ID theft prevention in *Company X* and *Company Z* (see Table 6.9).

6.4.2 Lack of Individual Staff Awareness

The existing literature shows that lack of individual awareness is a barrier in the process of knowledge sharing (see Section 2.5 in the literature review chapter). Individual staff member awareness is essential for the success of a knowledge sharing process in the organisation (Safa et al*.,* 2016). Lee and Al-Hawamdeh (2002) state that obligation of the significance of the knowledge would affect knowledge sharing between individuals, groups and teams in the organisations. Employee awareness of the knowledge sharing process encourages the individuals to share their knowledge effectively and provides the chance for creative thinking to handle complicated issues and understand the mistakes of others (Safa et al*.,* 2016). The literature clarifies that a lack of staff awareness is a barrier to knowledge sharing and it needs to be managed accordingly.

This research study found that there is a lack of awareness in the individuals and teams to share the knowledge for ID theft prevention in all the researched companies. A participant from *Company X* said:

> *"I do not know about the knowledge sharing for ID theft prevention."* (*Company X)*

Staff members from *Company Y* and *Company Z* are also not aware of the knowledge sharing process for ID theft prevention in their companies. Participants responded that:

> *"I do not know about the process of knowledge sharing. Nobody told me about it." (Company Y)*

> *"I am not aware of ID theft prevention knowledge sharing. Actually, we do not do it." (Company Z)*

Another participant said:

> *"I am not aware of identity theft. Well, I do not know about those problems." (Company Z)*

From the investigation of internal documents of all the researched companies, this study did not find any evidence of sharing knowledge for ID theft prevention. The main reason for not providing awareness to the staff members is that currently, companies are not

focusing on a knowledge sharing environment to enhance the awareness of staff for ID theft identification and protection from it. There is a lack of staff awareness to share knowledge for ID theft prevention. Therefore, it is a barrier in the process of knowledge sharing for ID theft prevention in the companies (see Table 6.9). This research agrees with the findings from the literature; online retail organisations need to increase the awareness of individual staff members regarding ID theft prevention and the process of knowledge sharing within the companies.

6.4.3 Insufficient Learning Opportunities

The literature review shows the importance of learning opportunities in the process of knowledge sharing in any organisation (see Table 2.13). According to Mohammad Hossein and Nadalipour (2016), a learning environment provides procedures leading to the increased capabilities and skills by routine work. The learning opportunities are a major factor in a successful knowledge sharing programme in any organisation (Cong & Pandya, 2003). There can be various learning opportunities to enhance the knowledge of staff members working in any organisation, and from those opportunities, training is effective to increase the knowledge of employees in the organisation. These are used to enhance technological skills for computer usage and knowledge sharing (Hortovanyi & Ferincz, 2015). Therefore, many organisations arrange different training opportunities for employees to keep them up-to-date and increase knowledge (De Grip & Sauermann, 2013; Dymock & McCarthy, 2006). According to Luu (2013) and Peter A.C. Smith (2012), the lack of a learning environment in an organisation is a barrier to enhancing the knowledge of individuals and teams.

The present study found that the researched companies have provided various learning opportunities to their staff members and training is one of those learning opportunities. The companies give training to new staff members to provide know-how about the existing infrastructure in the company and working procedures, such as how to interact with the computerised systems in the company, what the effective procedures are, and how to deal with customer data.

The researcher also found the availability of refresher courses to keep updated to the staff for new changes in the infrastructure, if the new system is implemented. However, this training is not provided to enhance a knowledge sharing environment for ID theft

prevention; only staff from the technical departments of the companies are offered the facility of training and refresher courses for ID theft prevention. At the moment, companies provide other learning opportunities for the workers, which include one-to-one meetings and seminars.

The present study agrees with the literature (see Section 2.5) that a lack of learning opportunities is a barrier in online retail organisations. Staff from non-technical departments of all these companies need further training to enhance their knowledge of ID theft issues and its prevention. Therefore, it is recommended that they provide learning opportunities to staff members working in the companies to strengthen their knowledge for ID theft prevention and to enhance knowledge sharing process for ID theft prevention within the companies (see Table 6.9).

6.4.4 Distrust of other Staff Members

According to Pan and Scarbrough (1998), an atmosphere of trust is necessary for the process of knowledge sharing in any organisation (Bălău & Utz, 2016; Hashim & Tan, 2015). Staff will work more efficiently if they trust other staff members working with them (Safa et al., 2016; Roth & Broad, 2008; Hsu et al., 2007; Bos et al., 2002; Ridings et al., 2002; Jones & George, 1998). Various empirical studies support the importance of trust for sharing knowledge in organisations (Rutten et al., 2016; Safa et al., 2016; Hsu et al., 2007). However, distrust can deter the implementation of knowledge sharing in an organisation (Willem & Buelens, 2009).

The current study found that in *Company X,* employees trust others within their department. They do not trust individual staff members or teams who work outside their department, and they are reluctant to share their knowledge of ID theft prevention with persons them. A participant from *Company X* responded:

> *"I cannot share knowledge with people who are not here in this department. I do not trust others outside my working unit." (Company X)*

Due to not having trust at the different department level, staff from non-technical departments are not getting the advantage of the knowledge sharing process for ID theft prevention within Company *X.* The lack of trust is a barrier to the process of knowledge sharing for ID theft prevention in the company.

The researcher found that knowledge regarding ID theft prevention is not a focus in Company *Y*. However, individuals trust each other to share their knowledge for regular jobs and day-to-day activities in the company. An interviewee from *Company Y* said:

> *"I trust people working there with me. I would like to discuss anybody working here in the company." (Company Y)*

Staff are willing to share knowledge with people either in their department or who work in any other department in *Company Y*. Another participant stated:

> *"There are no particular restrictions on sharing knowledge with other departments." (Company Y)*

There is no lack of trust in *Company Y,* but there is no knowledge sharing environment for sharing the knowledge for ID theft prevention. They need to enhance the knowledge sharing process for ID theft prevention in the company.

Employees in *Company Z* have trust at a departmental level. They share knowledge with others working individually, and in the teams within their departments in the company. However, staff working in technical departments do not trust the staff members working in non-technical departments of the company. Therefore, there is a lack of trust in *Company Z,* and it is a barrier in the process of knowledge sharing for ID theft prevention in the company.

Distrust is a barrier in the process of knowledge sharing for ID theft prevention within the organisation (see Table 6.9). The present study agrees with the literature for the need for the trust of other staff members for sharing the knowledge for ID theft prevention in the companies.

6.4.5 Fear of Information Leakage

Information leakage fear is a barrier in the process of knowledge sharing for ID theft prevention in online retail organisations. According to Abecassis-Moedas and Rodrigues Pereira (2016), growth in the problems of leakage of sensitive information issues has had considerable coverage in the media. Data leakage is becoming a main concern of the online retail companies and therefore it has attracted the attention of researchers (Huth et al*.,* 2013). Farahmand and Spafford (2013) emphasised various significant aspects of data leakage, which included insiders who leak valuable information.

The leakage of sensitive information through undisclosed channels is a challenging problem to manage in the organisations (Marabelli & Newell, 2012; Trkman & Desouza, 2012; Desouza, 2006; Desouza & Vanapalli, 2005). Table 2.15 in the literature review chapter shows that securing information is necessary for organisations and the fear of leakage of information is a barrier to knowledge sharing. Companies are very restricted in the protection of their resources and data.

From the investigation of the documents from these researched companies, this study found that they have strong rules and regulations to protect their information and resources. Due to these strict rules and policies, staff members have a fear of leaking information into the wrong hands. Staff members in *Company X* are not ready to share their knowledge for ID theft prevention with others working in the company. A participant said:

> *"I am afraid that others can leak the information I give them. So, I do not discuss with others for identity theft." (Company X)*

The researcher found that fear of information leakage is a barrier in knowledge sharing for ID theft prevention in *Company X*.

On the other hand, employees in *Company Y* have confidence in the information security infrastructure, and they do not fear leakage of information from outside attack on the IT systems in the company. A participant in *Company Y* said:

> *"We have good security infrastructure; we do not fear of leakage of information here." (Company Y)*

Staff are trusted and share their knowledge with each other, and therefore, fear of information leakage is not a barrier in the process of knowledge sharing in *Company Y*. However, the company needs to provide awareness of ID theft issues and its protection.

Employees in *Company Z* are strictly bound to the secure use of IT resources; therefore, it causes fear of information leakage to the staff members working in the company. An interviewee stated:

> *"I do not trust others. Anybody can leak the information. That is why we do not share security knowledge." (Company Z)*

Another respondent said:

> *"People are not trusted; they can steal information, I am afraid to share security knowledge." (Company Z)*

The fear of information leakage is a barrier in *Company Z,* and it impacts on the knowledge sharing for ID theft prevention in the company.

This study agrees with the literature findings. Individual staff members and teams working in the researched companies have a fear of information leakage which causes distrust in other employees working in different departments within their businesses. Therefore, it is a barrier in the process of knowledge sharing for ID theft prevention (see Table 6.9). Staff need to develop the confidence to share their knowledge for ID theft prevention and remove the fear of information leakage.

6.4.6 Insufficient Information Sourcing Opportunities and Inefficient ICT Infrastructure

The existing literature shows that an efficient process of knowledge sharing needs strong information sourcing opportunities and an efficient infrastructure of ICT in any organisation. Therefore, many organisations give importance to the availability of opportunities for information sourcing (Holsapple, 2013). Table 2.16 in the literature review chapter describes the need for sufficient information sourcing opportunities and an efficient ICT infrastructure for sharing the knowledge for ID theft prevention in an organisation.

From the investigation in all the researched companies, the researcher found various information sourcing opportunities were available to the staff. The existing ICT infrastructure in all the companies is good. However, existing information sourcing opportunities are not being used for the process of knowledge sharing for ID theft prevention in the companies, as they use the ICT infrastructure for their daily routine work and the communication of business tasks, and knowledge sharing for ID theft prevention is not in the focus of these companies (see Table 6.9). Therefore, there is a lack of information sourcing opportunities and ICT infrastructures used for knowledge sharing for ID theft prevention, and it is a barrier in the process of knowledge sharing for ID theft prevention in online retail organisations.

6.4.7 Lack of Leadership Support

The leadership of any organisation plays a vital role in managing the process of knowledge sharing (Muethel & Hoegl, 2016; Bass & Stogdill, 1990); therefore, it is their responsibility to practice strategic planning for the best use of resources and to enhance a learning culture and knowledge sharing in any organisation (Boerner et al., 2007). The leadership needs to bring about an open culture and to build an environment for knowledge sharing (Chuang et al., 2016) and therefore, top management must articulate the value of knowledge sharing. They should provide knowledge sharing approaches in the organisation (Mittal & Rajib, 2015).

The leadership of all of the researched companies is supportive. A participant from *Company X* stated:

> *"Management is good and helpful; they provide what we need here." (Company X)*

An interviewee from *Company Y* said:

> *"I am happy with the support of my managers." (Company Y)*

All the participants from *Company Z* were also satisfied with the support of their management. A respondent said:

> *"Our superiors always help us." (Company Z)*

This study found very supportive management in the researched companies and the staff are happy with them. However, there is no support from the leadership for a knowledge sharing process for ID theft prevention in their businesses. The present study agrees with the literature (see Table 2.17) about the need for leadership support for a knowledge sharing process for ID theft prevention in the organisation. The lack of leadership support is a barrier in the process of knowledge sharing for ID theft prevention (see Table 6.9).

6.4.8 Weak Knowledge Sharing Culture

Organisational culture refers to the shared values, beliefs and performances of persons within organisations (McDermott & O'Dell, 2001); therefore, it is one of the main elements considered in the organisation for knowledge sharing among the individuals as well as the teams; it needs to be understood in advance before employing any new strategies in the organisation (Syed-Ikhsan & Rowland, 2004). A knowledge sharing

culture is considered to be a significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM (see Table 2.18). Therefore, a weak knowledge sharing culture can be a barrier in the process of knowledge sharing in any organisation.

Currently, individual staff members and teams share knowledge with others working in their departments in *Company X.* A respondent said:

> *"We do not share knowledge with others, but we do share knowledge here in our department." (Company X).*

This study did not find a culture of sharing knowledge for ID theft prevention between different departments in *Company X;* due to that, there is a weak knowledge sharing culture in the company, and it is a barrier in the process of knowledge sharing for ID theft prevention.

On the other hand, *Company Y* has a strong culture of knowledge sharing. Staff members are trusted and share knowledge with each other in their department.

A participant responded:

> *"I trust my friends. Actually, we help each other in our department." (Company Y)*

There is a culture of knowledge sharing with employees working in different departments within the company and staff trust other employees working outside their department. Another participant said:

> *"We have a good culture of information sharing. We are quite good at trusting others. Well, I can trust all staff here working in this company, and I should do it as others trust me." (Company Y)*

Individual staff members are willing and happy to share knowledge with others in their team or department and with the persons working outside their departments within the company. However, this study did not find a culture of knowledge sharing for ID theft prevention. Staff are not sharing the knowledge of ID theft prevention, and therefore it is a barrier in the process of knowledge sharing for ID theft prevention in *Company Y.*

This investigation found that *Company Z* has a culture of knowledge sharing at the departmental level. An interviewee in the company stated:

> *"I share what I do here in my department. Others also do it here." (Company Z)*

Staff members do not share knowledge with employees working outside their department in the company.

A respondent said:

> *"... we do not discuss with others who do not work with us." (Company Z)*

The present study found that *Company Z* has a weak culture of knowledge sharing. This study agrees with the findings from the literature review (Section 2.5) that weak knowledge sharing culture is a barrier in the process of knowledge sharing for ID theft prevention within an organisation. There is a need for a strong culture of knowledge sharing for ID theft prevention in the online retail organisations (see Table 6.9).

6.4.9 No Job Rotation

Job rotation plays a vital role in enhancing the knowledge of individual employees and teams within and outside any department in an organisation (Aga et al., 2016; Huang & Pan, 2014; Ortega, 2001). Table 2.19 describes the need for job rotation in the process of knowledge sharing in an organisation.

The present study did not find any job rotation process in *Company X,* and all participants responded with *"No Job rotation"*. The lack of job rotation in the company causes a barrier in the process of knowledge sharing and not enhancing the knowledge of individual staff members and teams in the business. Not rotating jobs leaves the individuals to learn from their own experiences and is a barrier to knowledge sharing for ID theft prevention in the organisation.

On the other hand, *Company Y* has strong job rotation; employees are getting the advantages of job rotation to increase their knowledge while working in different teams and departments in the company. They learn about new systems which were not used in previous departments and learn from the experiences of other departments. Staff are happy and also learn in the form of doing something new with a different job role and experience new things. A participant stated:

> *"I am happy to work with the new environment and new people. I learn from them, and it leaves me no chance of failure. So I am happy with it." (Company Y)*

Another respondent said:

> *"It is useful for gaining knowledge of different areas of the company." (Company Y)*

However, the company is not rotating the jobs to increase the knowledge of persons for ID theft identification and its prevention. Therefore, job rotation does not play any role to enhance the knowledge of individuals in the company for ID theft prevention. Departments are not getting the advantage of knowledge sharing for ID theft prevention from the people of other departments. Therefore it is a barrier in knowledge sharing for ID theft prevention in *Company Y*.

Company Z is also not rotating the jobs of individuals; from the investigation of the internal documents, the research did not find any evidence of a job rotation process in the company. During the interview a participant said:

> *"We do not have any policy of job rotation in the company here." (Company Z)*.

Staff are learning from their own experiences.

From the responses of the participants, the researcher found that staff are learning from their own experiences and doing the same jobs over years of working in the company.

Another respondent said:

> *"I gain knowledge from my things I experience here, and I do not need to go anywhere and ask how to do my work." (Company Z)*

The literature clarifies that job rotation is important for enhancing the knowledge of employees to prevent ID theft and share the knowledge for ID theft prevention. Table 2.19 shows that job rotation increases the knowledge of individuals, and enables employers to find out the employees' strengths and weaknesses. Therefore, this study agrees with the literature findings, that the lack of job rotation causes no enhancement to the knowledge of individuals and teams in the organisation in the researched companies. Not rotating jobs leaves the individuals to learn from their own experiences and is a barrier to knowledge sharing for ID theft prevention in the organisations.

Table 6.9 Barriers to knowledge sharing for ID theft prevention in the organisations

Barrier in KS	Literature Findings	Empirical findings (Barrier in KS)			Recommendations of this Study
		Company X	*Company Y*	*Company Z*	
Staff unwillingness	Yes	Yes	No	Yes	The organisations should focus on the staff willingness of knowledge sharing for ID theft prevention.
Lack of individual staff awareness	Yes	Yes	Yes	Yes	The companies should enhance the individual staff awareness for sharing the knowledge for ID theft prevention.
Insufficient learning opportunities	Yes	Yes	Yes	Yes	There is a need for enhancing learning opportunities for the awareness of individual staff and teams to share the knowledge for ID theft prevention within companies.
Distrust of other staff members	Yes	Yes	No	Yes	The companies should increase the trust level at the different department level. Employees need to trust others to share the knowledge for ID theft prevention within the companies.
Fear of information leakage	Yes	Yes	No	Yes	Companies need to develop the confidence of staff members to share their knowledge for ID theft prevention. They need to educate staff members to remove the fear of information leakage.
Insufficient information sourcing opportunities and inefficient ICT infrastructure	Yes	Yes	Yes	Yes	Companies should use existing information sourcing opportunities and ICT infrastructure for sharing the knowledge for ID theft prevention with companies. Further information sourcing opportunities are required to enhance the knowledge of staff in the companies.
Lack of leadership support	Yes	Yes	Yes	Yes	The leadership of the companies must support the implementation of a knowledge sharing process for ID theft prevention in the companies.
Weak knowledge sharing culture	Yes	Yes	Yes	Yes	Companies need to increase the knowledge sharing culture for ID theft prevention across the company.
No job rotation	Yes	Yes	Yes	Yes	The companies need to develop a process of job rotation across the departments within the organisations.

Table 6.9 describes the barriers in the process of knowledge sharing for ID theft prevention in the organisations. Staff unwillingness, lack of individual staff awareness, insufficient learning opportunities, distrust of other staff members, fear of information leakage, insufficient information sourcing opportunities and inefficient ICT infrastructure, lack of leadership support, weak knowledge sharing culture, and no job rotation are barriers in the process of knowledge sharing for ID theft prevention in online

retail organisations. It describes the literature findings for the availability of barriers. It also describes the existence of barriers in the three researched companies. Table 6.9 also includes the recommendations of this study for the removal of existing barriers in the process of knowledge sharing.

6.5. Unique Contribution of This Research

The literature review identified that ID theft is a major problem for the online retail sector. Employees working in online retail organisations need to enhance their knowledge of ID theft identification and its prevention. The knowledge of employees can be improved through sharing their knowledge for ID theft prevention. Through the process of research refinement, this study could not find previous research work on the investigation of knowledge sharing processes for ID theft prevention in online retail organisations, which leaves a research gap in the area of study. The present study makes a new contribution which makes it unique. This study has investigated the knowledge sharing process for ID theft prevention within online retail organisations. The researcher studied and analysed ways in which individual staff share their knowledge for ID theft prevention with each other, investigated the knowledge sharing process between teams within and outside departments in organisations, and identified existing barriers in knowledge sharing for ID theft prevention in organisations. This study also extended a guiding framework for improving the knowledge sharing process for ID theft prevention inside the organisations. The following section includes the extension of the framework for knowledge sharing processes for ID theft prevention in the online retail sector.

6.5.1. Extended Framework for Knowledge Sharing Processes for ID Theft Prevention in Online Retail Organisations

This study has extended the framework in two ways: one is the extension of a guiding framework in the context of knowledge sharing processes for ID theft prevention; the second is making amendments to the guiding framework which is discussed as follows:

- **Use of Framework in a New Research Context**

After comparing and contrasting in terms of knowledge sharing and ID theft prevention and the further criteria of selecting an appropriate framework for extension (Chapter 3), the framework proposed by Salleh (2010) was selected as the guiding framework for data

collection (see Section 3.4). The framework was adopted for extension in the context of the present study. It was also previously used by Siong et al. (2011) for KM implementation in a public sector organisation. It was comprehensive in order to investigate the knowledge sharing process and was capable of fulfilling the research objectives for the present study. The framework was flexible and could be modified for the purpose of this study as it covered the major factors of knowledge sharing and was not too complex to adopt for an extension. It was useful for ongoing improvements; for example, it enables knowledge sharing within an organisation as it connects KM enablers and the process to share knowledge in a public-sector accounting organisation. The framework includes the components having a clear focus in the present study. It interconnects solutions of KM through culture, leadership, learning and technology to enhance a knowledge sharing process in the organisations, which was the main focus of the present study as it is the investigation of knowledge sharing processes for ID theft prevention. Moreover, it was better focused on ongoing improvements as it enables knowledge sharing processes and is useful as a process of strategic KM which supports knowledge networks and knowledge flow to enhance the decision-making process in the organisations.

The guiding framework was not used to enhance knowledge sharing processes for ID theft prevention. Therefore, the framework has been extended in the context of improving knowledge sharing processes for ID theft prevention within the online retail organisations (see Figure 6.3). The researcher published a separate research article on the extended framework during the process of this study (Abdullah et al. 2016).

- **Amendments in Guiding Framework for Effective Knowledge Sharing Processes for ID Theft Prevention**

The amendments in the guiding framework included the removal of unnecessary factors in the context of the present research study. The present study adds new factors useful for effective knowledge sharing processes for ID theft prevention. Furthermore, important and relevant topics were borrowed from the guiding framework to fulfil the requirements of this study; for example, job rotation, feedback on performance evaluation, information sourcing opportunities, leadership support, and a knowledge sharing culture are adopted from guiding framework.

However, the factors such as know-how and skills, job training, and learning opportunities were replaced by the factors ICT know-how and training. The existing literature notes that job training is being given for the improvement of working procedures. Job training is useful to enhance knowledge only in the workplace in the current organisation. This training is provided to improve the knowledge about the machines, and to understand the infrastructure of the workplace and procedures which are used only within the firm where the employee is working, which can be provided to

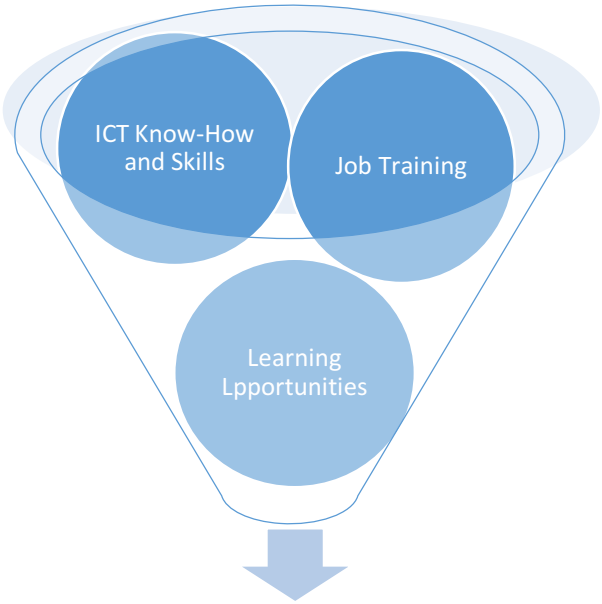

Figure 6.1 ICT Know-How and Training - an extended factor

gain knowledge about particular characteristics of the products and customers of the organisation or firm (De Grip & Sauermann, 2013).

Employees receive training according to the nature of their work and thus enhance their working knowledge which is out of the scope of this study. However, in the knowledge sharing process for ID theft prevention, training is required in the companies to enhance the knowledge sharing processes for ID theft prevention. Therefore the factor job training needs to be replaced with a new knowledge enabler which is useful for an effective knowledge sharing process for ID theft prevention within the online retail organisation.

Furthermore, in the guiding framework, ICT know-how, job training and learning opportunities factors make it complicated and difficult to implement in the context of knowledge sharing for ID theft prevention. During the investigation for this study, the researcher found that training is one of the learning opportunities required to enhance the knowledge of individual staff members and teams for knowledge sharing for ID theft prevention within and outside the department in the organisation. Therefore, these factors cannot be separated to provide the knowledge for ID theft prevention and need to be replaced by a new factor of ICT know-how and training. Therefore, the complicated and unnecessary factors are replaced by a new factor. Figure 6.1 shows the replacement of

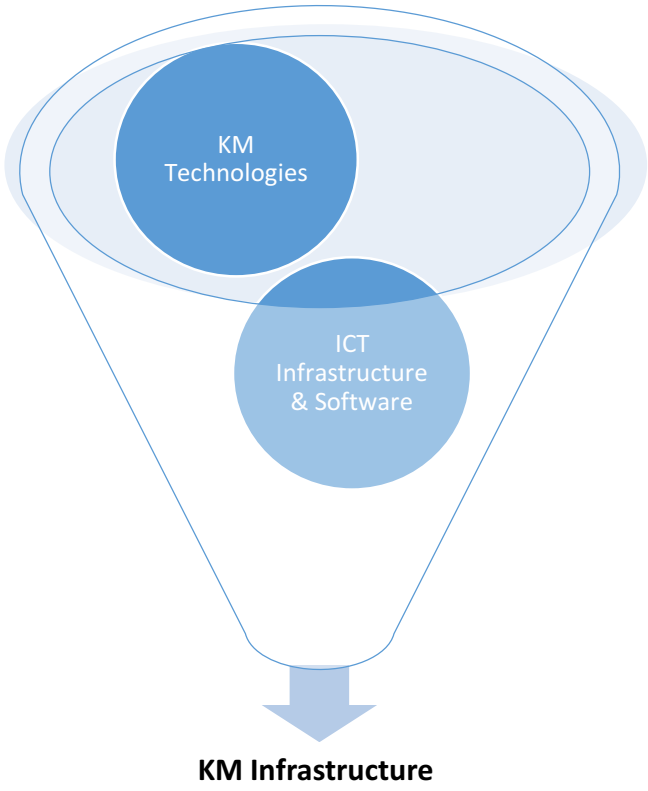

Figure 6.2 KM Infrastructure - an extended factor

unnecessary and complicated factors (ICT know-how, job training and learning opportunities) with ICT know-how and training factor (new factor).

Furthermore, the guiding framework includes ICT infrastructure and software, and KM technologies factors. However, this study found that ICT infrastructure and software is a part of KM technologies and cannot be separated for knowledge sharing for ID theft prevention. Having these separate factors in the framework makes it more complex for the individuals and teams to share their knowledge of ID theft prevention and needs to be replaced by a new factor which makes the framework easy to understand and implement

to enhance the knowledge sharing processes for ID theft prevention. Therefore, the researcher replaced both factors with a new KM infrastructure factor. Figure 6.2 shows the replacement of the factors with a new factor.

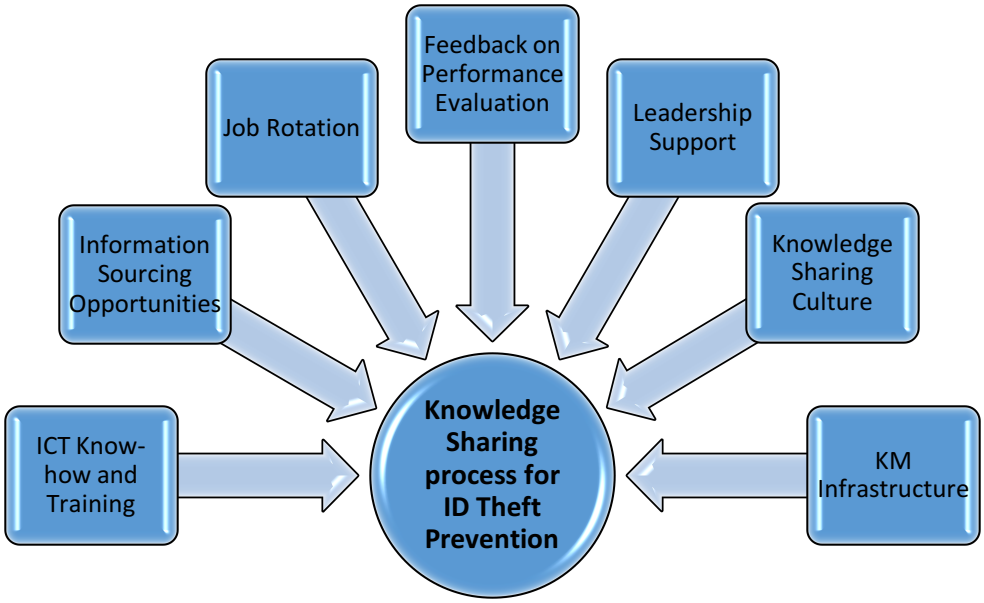

Figure 6.3 Knowledge sharing processes for ID theft prevention within organisations (extended framework proposed by Salleh (2010))

6.5.2. New Lessons Learned from this Study

The new lessons learnt from this study make it novel and contribute to the existing area of research. Through the investigation, the research found that the knowledge sharing process for ID theft prevention needs to be enhanced. Existing barriers to the knowledge sharing for ID theft prevention within online retail organisations were identified. The new lessons learnt from this study are discussed below.

- **Individual Staff Members' Knowledge Sharing**

The present study contributes to understanding the role of individual staff members to share their knowledge of ID theft prevention within the organisation. It also provides the understanding of the need and availability of knowledge sharing factors to prevent ID theft within online retail organisations. The findings of this study illustrate that knowledge of ID theft prevention is not being shared between individual staff members across the departments in the companies. Staff share knowledge of ID theft prevention

within their own departments. Basic training is being given to fresh members of staff to provide them with the know-how about the systems used and the working activities within the companies.

One of the companies researched arranges seminars on ID theft prevention. Online retail companies need to develop an educational system to enhance the knowledge of employees in ID theft prevention knowledge sharing. Online retail companies disseminate some policy documents to individual staff members on ID theft prevention which set out awareness of confidential information, but these documents do not describe knowledge sharing for ID theft prevention. Staff use e-mails to share their knowledge for their working activities.

There is no job rotation for enhancing the knowledge of individual staff members regarding ID theft prevention. Employees learn from their own experience, which is time-consuming and exhaustive. On the other hand, one of the researched companies has a job rotation process, but it is not being used to enhance the knowledge of staff about the ID theft prevention. Job rotation in organisations is important to enhance the knowledge of individual staff members. The companies need to rotate the knowledge holders' jobs across various departments to enhance the knowledge of other staff members on ID theft prevention. Individual staff members trust others within their own department and share knowledge with them regarding preventing ID theft. They need to enhance the trust level across other departments for ID theft prevention knowledge sharing.

- **Knowledge Sharing Process Between Teams in Different Departments**

The present study found the existing KM infrastructure is not being used to share knowledge for ID theft prevention among the teams working in different departments in online retail organisations. The knowledge sharing tools are not being used for the knowledge sharing for ID theft prevention at different departmental levels. Teams working in different departments are not getting the advantage of the existing KM infrastructure to enhance their knowledge for ID theft prevention. Therefore, the organisations should design and implement an effective KM infrastructure for knowledge sharing for ID theft prevention between different departments. The literature gives importance to learning opportunities to enhance the knowledge of individual staff members and teams working across different departments in organisations (see Chapter 2). However, the present study found all three researched companies provide very basic training to staff newly joining the company. The companies provide training to the staff

according to their job role and to understand the tools they use for their work. There is no specific training available to the staff that includes ID theft prevention awareness in any of the researched companies. The team members working in non-technical departments particularly need awareness of ID theft problems and how to protect against these issues. Therefore, the organisations should design a comprehensive ICT know-how and training programme to educate the staff to share ID theft prevention knowledge in different departments.

The literature shows that job rotation enables individuals to learn from various departments, decreases employee exhaustion caused by tedious or boring job tasks, and increases both an individual's confidence and their satisfaction in the job (Eriksson & Ortega, 2006; H. Huang, Liao, & Thou, 2005; Kampkötter, Harbring, & Sliwka, 2016; Triggs & King, 2000). It plays an important role in enhancing the knowledge of employees to prevent ID theft and share their knowledge for ID theft prevention (Kane et al., 2005). The present study found that there is no job rotation process in *Company X* and *Company Z*. *Company Y* has a job rotation process, but it is not being used to enhance the knowledge of individual staff members to share their knowledge of ID theft prevention in the company. Therefore, online retail organisations should introduce a job rotation process to enhance the knowledge of individuals and teams working in different departments.

Current developments in computerised technology are advancing the nature of monitoring the performance of employees (Alder & Ambrose, 2005). Feedback is vital for the evaluation and monitoring of activities of employees. It can be given for various purposes which include bringing the outcomes of activities or processes into focus; providing information when workers move away from primary goals; helping to fix new goals or adjusting the existing goals; and guidance to perform the activities. It also promotes critical reflection and brings about new approaches (Gabelica et al., 2012).

All of these researched companies evaluate the performance of staff. Managers hold monthly meetings with employees and provide them with feedback on their performance. However, the present study did not find the process of feedback on performance evaluation for knowledge sharing for ID theft prevention in any of these organisations. The organisations need to implement an employee evaluation process and provide feedback to staff working individually or in teams in different departments, for effective knowledge sharing for ID theft prevention.

It is important for organisations to consider information as a resource in their organisation (Holsapple, 2013). Substantial procedures for making organisational learning or knowledge available by expediting knowledge sharing among the proficient workforce are essential (Bhatt et al., 2010; Khan et al., 2016). Information sourcing opportunities or ease of gaining information is vital for knowledge sharing for ID theft prevention among the teams in different departments. Consistent contact or communication networks with proficient information or a degree of technical and professional knowledge that is easily obtainable and available to employees are specimens of information sourcing opportunities.

All three companies provide different information sourcing opportunities in their company and share required knowledge with others within the working environment. However, the online retailers are not concentrating on the awareness of ID theft issues and its prevention with their staff. Existing information sources can be used for sharing knowledge of ID theft prevention inside the companies. The teams and departments can avail themselves of these opportunities to enhance their knowledge of ID theft identification and its prevention. Therefore, the online retail organisations need to enhance information sourcing opportunities and use them for knowledge sharing for ID theft prevention between different departments in the organisation.

The literature shows that leadership has an important role in managing the knowledge sharing process in any organisation (Bass & Stogdill, 1990; Muethel & Hoegl, 2016). It is accountable for practising strategic planning for best use of means and promoting a learning culture and knowledge sharing (Boerner, Eisenbeiss, & Griesser, 2007). The present study found a supportive leadership in the researched companies, where staff are happy with their management. However, there is the need for an enhanced environment for knowledge sharing for ID theft prevention. Leadership support is required to develop an educational environment for enhancing the knowledge of ID theft prevention and sharing its knowledge across different departments in the organisation. Their support is needed by the individual staff members and teams in order to share the knowledge of ID theft prevention in the organisations.

According to Stoddart (2001), knowledge sharing can work if the culture of the organisation supports it, and changes need to be developed according to the culture of the organisation, as having a weak culture of knowledge sharing causes hurdles to the knowledge sharing process. Therefore, it needs to be managed for an effective knowledge

sharing process in the organisations. This study found that *Company X* and *Company Z* have a knowledge sharing culture only at the departmental level, and staff are trusted at the departmental level. However, individual staff members and teams are not ready to share their knowledge with others outside their department within their company. While talking about *Company Y*, this study found a good culture of knowledge sharing where staff are ready to share their knowledge with anybody working outside their department in the company. However, there is no culture of knowledge sharing for ID theft in *Company Y,* and therefore it is recommended that the organisations develop a culture of knowledge sharing for ID theft prevention between different departments in the organisations. The trust of other staff members working in non-technical departments should be increased for knowledge sharing for ID theft prevention within organisations.

- **Barriers to the Knowledge Sharing for ID Theft Prevention**

The present study also contributes by identifying the barriers to the process of knowledge sharing for ID theft prevention in online retail of the UK. It provides solutions to help remove the existing barriers and to create an effective knowledge sharing process for ID theft prevention within online retail organisations. It identified staff unwillingness, lack of individual staff awareness, insufficient learning opportunities, distrust of other staff members, insufficient information sourcing opportunities, inefficient ICT infrastructures, lack of leadership support, a weak knowledge sharing culture, and no job rotation are the barriers to the process of knowledge sharing for ID theft prevention in online retail organisations. Online retail organisations need to remove the existing barriers to the process of knowledge sharing for ID theft prevention.

As discussed earlier in the literature review chapter, staff willingness is a significant element in the process of knowledge sharing. From the investigation, this study found that it is a barrier to knowledge sharing for ID theft prevention in online retail organisations. Staff members in two of the researched companies are not willing to share their knowledge of ID theft prevention. Therefore, online retail organisations should focus on the staff willingness to share knowledge for ID theft prevention.

Individual staff awareness is one of the most important elements in the process of knowledge sharing. However, workers in online retail organisations are not sufficiently aware of the knowledge sharing process for ID theft prevention and its importance. They require the awareness for an effective knowledge sharing process for ID theft prevention.

Therefore, the companies should enhance individual staff awareness for ID theft prevention and its knowledge sharing within the organisation.

The literature adds the importance of having sufficient learning opportunities to enhance the knowledge of staff working in the organisations. This research found that there are enough learning opportunities for employees in the online retail companies. However, these learning opportunities are not being used to share the knowledge for ID theft prevention. There is a need to enhance the learning opportunities to raise the awareness of individual staff and teams to share their knowledge for ID theft prevention within companies.

The literature clarifies that trust is the main element in the process of knowledge sharing. The present study found that employees in two of the three researched companies share their knowledge with others within their working department, but they are not sharing knowledge of ID theft prevention with others working outside their department within the companies. Staff do not trust sharing their knowledge. The lack of trust of other staff members is a barrier to knowledge sharing for ID theft within online retail organisations. Therefore, it needs to be managed for an effective knowledge sharing process in the organisations. The companies should increase the trust level at different departmental levels. Staff need to trust others working in different departments within the organisation and share their knowledge of ID theft prevention with them.

While talking about inefficient ICT infrastructure and sufficient information sourcing opportunities, they are very important for any organisation when handling its information. The lack of an ICT infrastructure and information sourcing opportunities are barriers to knowledge sharing. This study found that online retail companies have a good communication infrastructure and sufficient information sourcing opportunities. However, these are not being used to share knowledge for ID theft prevention, which is a barrier to the knowledge sharing for ID theft prevention. Companies should use their existing information sourcing opportunities and ICT infrastructures to share the knowledge of ID theft prevention within companies. Further information sourcing opportunities are required to enhance the knowledge of staff in the companies.

The existing literature shows the importance of the role of leadership in managing the knowledge sharing process in any organisation (Muethel & Hoegl, 2016; Bass & Stogdill, 1990). The leadership is accountable for practising strategic planning for best use of the

means and promotion of a learning culture of knowledge sharing. The leadership needs to bring in an unrestricted culture and to build an environment for knowledge sharing (Chuang et al., 2016). However, this study found that a lack of leadership support is a barrier to the knowledge sharing for ID theft prevention in the online retail organisations. Therefore, the support of leadership is required for individual staff members and teams to share their knowledge of ID theft prevention in the organisations.

According to Stoddart (2001), knowledge sharing can work if the culture of the organisation supports it, but changes need to be developed according to the culture of the organisation, as having a weak culture of knowledge sharing causes hurdles to the knowledge sharing processes. At the moment, the online retail companies are lacking a strong culture of knowledge sharing for ID theft prevention within their organisations, which is a barrier to knowledge sharing for ID theft prevention within online retail organisations. Therefore, the current study recommends that online retail organisations should develop a culture of knowledge sharing for ID theft prevention at different department levels. The trust of other staff members working in non-technical departments should be increased for ID theft prevention knowledge sharing in the organisations.

Job rotation is vital for increasing the knowledge of individual staff and different teams within and outside any department within an organisation. There is a need for job rotation to enhance the knowledge sharing process for ID theft prevention. However, from the investigation of the researched companies, this study found that there is no process of job rotation for knowledge sharing for ID theft prevention within the companies. The study also found that having no job rotation is a barrier to the process of knowledge sharing for ID theft prevention in online retail organisations. Online retail organisations should utilise a process of job rotation to enhance the knowledge of individuals and teams working in different departments of the organisation.

6.5.3. Contribution of Investigating the Online Retail Sector

The online retail sector investigated in the context of knowledge sharing processes for ID theft prevention also makes this research new, having a novel contribution in the area of existing research. The researcher identified existing barriers to knowledge sharing for ID theft prevention in online retail organisations, and found the weaknesses of the companies were in individual staff learning, regarding an effective knowledge sharing process to prevent ID theft. This study provided a framework for knowledge sharing for ID theft

prevention within online retail organisations. It helps the retail industry to enhance the process of knowledge sharing for ID theft prevention in organisations and provides solutions for developing a knowledge sharing culture at different departmental levels in a company. Guidance is suggested to develop an educational environment for spreading knowledge of ID theft prevention and how to share it with staff members within a company.

This study guides the leadership regarding managing existing resources for an effective learning environment for knowledge sharing for ID theft prevention in their companies. The researcher provided the case study report to the management of the participating companies. The case study reports were produced from the findings of their own participating company. Furthermore, a cross-case report was provided with each of the researched companies for the guidance of management to remove the existing barriers and weaknesses in the process of knowledge sharing for ID theft prevention and strengthen the process of knowledge sharing for ID theft prevention and its awareness.

6.6. Recommendations for Improving Knowledge Sharing Processes for ID Theft Prevention within Organisations

1. From the review of the existing literature in the area of research, this study found that there is a need for KM infrastructure to share knowledge for ID theft prevention in the organisations. However, the current study did not find the use of an existing KM infrastructure in all the researched companies for knowledge sharing for ID theft prevention within the companies (see Table 6.8). Therefore, the online retail organisations should design and implement an effective KM infrastructure for knowledge sharing for ID theft prevention.
2. A learning environment leads organisations to the height of success. It defines procedures leading to the accumulation of capabilities and skills through routine work (Mohammad Hossein & Nadalipour, 2016), which is the priority of many enterprises who consider themselves to be continuous learning organisations to enhance the potential of their workers for the sake of competitiveness in the global market. Learning opportunities enhance the progress in outcomes by removing previous mistakes and weaknesses in organisations (Harteis et al*.,* 2008). Table 2.13 describes the need for learning opportunities in the organisation. This study found all three researched companies provide very basic training to staff newly

joining the company. The companies provide training for the staff for their job role and the tools they use for work. However, there is no training available to the staff that includes ID theft prevention awareness in any of the researched companies, particularly for the staff members working in non-technical departments in these companies (see Table 6.8). Therefore, it is recommended that online retail organisations must design a comprehensive ICT know-how and training programme to educate their individual staff members and teams in knowledge sharing for ID theft prevention within the companies.

3. Job rotation is vital to increase the knowledge of individual staff and different teams within and outside any department within an organisation. Table 2.19 in the literature review chapter shows that there is a need for job rotation to enhance the knowledge sharing process for ID theft prevention. However, from the investigation of the researched companies, this study found that there is no process of job rotation for knowledge sharing for ID theft prevention within the companies (see Table 6.8). The study also found that having no job rotation is a barrier in the process of knowledge sharing for ID theft prevention in online retail organisations (see Table 6.9). Online retail organisations should enable the process of job rotation to enhance the knowledge of individuals and teams working in different departments within the organisations.
4. Current developments in computerised technology are advancing the nature of monitoring the performance of employees (Alder & Ambrose, 2005). However, the existing literature gives importance to feedback on employee performance, which is necessary for any organisations. It can be given for various purposes, for example, bringing the resultant outcomes of the activities or the processes into focus; providing information when workers move away from primary goals; helping them to fix new goals or adjusting the existing goals, and providing guidance for performing their activities. The feedback also promotes critical reflection and brings about new approaches (Gabelica et al., 2012). However, this study did not find any feedback on performance evaluation for knowledge sharing for ID theft prevention (see Table 6.8). Therefore, online retail organisations should implement an employee evaluation process and provide feedback to them on effective knowledge sharing for ID theft prevention within the companies.
5. The literature emphasises the availability of information sourcing opportunities for knowledge sharing (see Table 2.16). An effective process of knowledge

sharing needs well-structured information sourcing opportunities in any organisation. Therefore, it is important for organisations to consider information as a resource in the organisation (Holsapple, 2013). Consequential methods of making organisational learning or the knowledge available by expediting the process of knowledge sharing among the skilled workforce are inevitable (Bhatt et al*.,* 2010; Khan et al*.,* 2016). Therefore the availability of information sourcing opportunities are necessary for knowledge sharing for ID theft prevention among individual staff members and teams. However, this study found that existing information sourcing opportunities are insufficient for an effective knowledge sharing process for ID theft prevention within online retail organisations (see Table 6.8). Therefore, the present study recommends enhancing information sourcing opportunities and using them for knowledge sharing for ID theft prevention in the organisations.

6. The existing literature notes the important role of leadership in managing the knowledge sharing process in any organisation (Muethel & Hoegl, 2016; Bass & Stogdill, 1990). Table 2.17 shows that it is accountable for practising strategic planning for best use of the means and promotion of a learning culture and knowledge sharing, along with the leadership required to bring about an unrestricted culture and to build an environment for knowledge sharing (Chuang et al*.,* 2016). This study found that lack of leadership support is a barrier in knowledge sharing for ID theft prevention in the online retail organisation (see Table 6.9). Therefore, this study recommends the support of leadership for individual staff members and teams to share their knowledge for ID theft prevention in the organisations.
7. According to Stoddart (2001), knowledge sharing can work if the culture of the organisation supports it, but changes need to be developed according to the culture of the organisation, as having a weak culture of knowledge sharing causes hurdles to the knowledge sharing process (see Table 2.18). Therefore, it needs to be managed for an effective knowledge sharing process in the organisation. This investigation found that employees in two of the three researched companies share their knowledge with others within their working department. Staff members are not sharing the knowledge for ID theft prevention with others working outside their department within the companies. Staff members are not trusted to share the knowledge for ID theft prevention. Therefore this study recommends that online

retail organisations should develop a culture of knowledge sharing for ID theft within the organisation. The trust of other staff members working in non-technical departments should be increased to share their knowledge for ID theft prevention in the organisations.

6.7. Chapter Summary

This chapter included the analysis and discussed the data collected from three online retail organisations in the UK. The research study extended the knowledge sharing framework proposed by Salleh (2010) using the theory of KM. The research themes have been adopted from the guiding framework, and this study created new themes to fulfil the requirements of the investigation which provided a framework for knowledge sharing for ID theft prevention in the organisations.

The collected data from all three researched online retail organisations were analysed using thematic analysis methods. A cross-case comparison was undertaken for the three case studies which were completed in this research study. The findings were analysed and discussed for every theme of this study in these three cases.

This study found that online retail industry organisations are not good enough at the process of knowledge sharing for ID theft prevention in their organisations; they provide awareness of their working activities and provide various knowledge sharing facilities to enhance their working knowledge. However, none of these three companies focus on the awareness of a knowledge sharing environment for ID theft prevention. Only one of the researched companies has a knowledge sharing process at different department levels; the other two researched companies do not share knowledge outside the departments within the companies.

Staff members are not trusted to share their knowledge for ID theft prevention. Non-technical staff members from all these companies do not have an awareness of ID theft issues and its prevention, and they require an educational environment for know-how on these issues and how to protect against them. The present study identified existing barriers in knowledge sharing for ID theft prevention and provides solutions to remove these barriers. The current research study has bridged an existing gap by the novel contribution in the area of knowledge sharing for ID theft prevention and has extended a knowledge sharing framework to enhance the knowledge sharing process for ID theft prevention in

online retail organisations. It also contributed to the online retail organisations by providing a suitable framework and guidance for the management of the companies to enhance the awareness of the knowledge sharing process for ID theft prevention within the companies.

The companies are strongly advised to implement a knowledge sharing process for ID theft prevention. They must encourage individuals and teams to share their knowledge with staff outside their department. Knowledge sharing cultural enhancement is needed so that workers can trust sharing their knowledge for ID theft prevention.

CHAPTER 7 CONCLUSION

7.1. Research Summary

The literature review did not find any evidence of research undertaken on knowledge sharing process for ID theft prevention in online retail organisations. The literature includes research on ID theft prevention and organisational knowledge sharing in the organisations separately. However, it was necessary to investigate the online retail sector in the context of this research study.

The aim of this research was to investigate and analyse the sharing process within an online retail organisation and to extend a knowledge sharing framework to improve the knowledge sharing process for ID theft prevention. Bearing this in mind, the research questions posed in Chapter 1 were developed.

Theory of knowledge was used to structure the literature review in the related area of research. Various frameworks in the area of ID theft prevention and knowledge sharing were studied and compared under the selected factors of the research study (see Section 3.3). By comparing and contrasting, a knowledge sharing framework proposed by Salleh (2010) was adopted for extension in the context of knowledge sharing for ID theft prevention in the online retail organisation (see Section 3.4). The guiding framework has already been applied in other industries in the context of knowledge sharing.

This study used qualitative research methods based on case study research. The researcher conducted three case studies at different levels of online retail companies in the UK. The methods of data collection included semi-structured interviews and internal and external document analysis. The researcher adopted the thematic analysis method for analysing the collected data using NVivo software tools for research analysis along with a manual coding process.

The total number of semi-structured interviews was 34, and the length of time was between 45 to 75 minutes each. The participants were selected from top management to lower level staff from both technical and non-technical departments in the researched companies.

The investigation of the documents included external documents, which were collected from different sources; for example, online retail industry reports published in various

industry magazines, journals and conference proceedings, electronic and printed media reports, and reports published on the researched company websites. Additionally, the researched companies provided internal documents for the investigation, including policy documents, short memos and email conversations. Ethical approval for data collection was sought from the parent university.

The researcher approached the first company for data collection through the Director of Studies for the first case study of this research. An agreement of confidentiality was signed by the researcher and the management of the company (*Company X*). The company provided 14 semi-structured interviews and internal documents. For the further two case studies, various online retail companies were approached. Two of the companies approached agreed to provide access to data collection; one (*Company Y*) of these two companies allowed the investigation of internal documents, along with interviews. The researcher conducted 13 semi-structured interviews along with internal documents. The third company (*Company Z*) provided 7 semi-structured interviews and internal documents. The data collected from each company was analysed separately using thematic analysis. In addition, the cross-case analysis was undertaken for all three case studies in the researched companies.

7.2. Research Objective 1: To study and analyse ways in which individual staff share their knowledge of ID theft prevention

From the investigation, this study found various ways in which individuals share knowledge with each other. They use different methods of communication, for example, they use email conversations and a corporate social networking system they call 'Yammer'. The researched companies have their own knowledge sharing environment, such as *Company X* uses a page they call 'Blackboard' where they post updates for individuals, and *Company Y* uses SharePoint 2007 and an e-portal to share information.

The companies have different learning procedures for individuals; for example, they arrange inductions for newcomers, have scheduled training programs and arrange seminars and street shows. All these opportunities are being provided to individuals for know-how and awareness of the working environment and usage of the existing facilities which include the IT infrastructure and working procedures.

Company Y is open for conversation and sharing the knowledge of individuals within and outside their departments. However, the individuals from *Company X* and *Company Z* share their information with others within working departments; they are reluctant to share their information with individuals outside their working departments.

The leadership is supportive in all three companies, communicating with staff through emails, phone calls and meetings. At the departmental level, managers arrange meetings with staff to discuss progress and working tasks. Line managers walk to the desks of the individual staff members and discuss any issues with them. Individual staff members get feedback from management through emails and one-to-one meetings.

At the moment, individual staff members from the information security and fraud prevention departments share their knowledge for ID theft prevention in *Company X* and *Company Z*. However, there is no knowledge sharing process for ID theft prevention between the individuals in non-technical departments in all three researched companies. Existing learning opportunities are not being used to enhance the knowledge of individuals. Companies need to increase the trust level among individuals regarding sharing their knowledge for ID theft prevention. Individuals need to enhance their knowledge of the knowledge sharing process for ID theft prevention in their companies.

7.3. Research Objective 2: To investigate the knowledge sharing processes for ID theft prevention between teams within and outside departments in organisations

Staff members in the online retail organisations are working in teams and groups, and they share their knowledge with each other in their own departments, helping each other and completing the working tasks in the group. They are learning from the experiences of their team members and enhancing their knowledge.

Teams in the technical departments of *Company X* and *Company Z* work on securing the organisational and customers' knowledge. Therefore, team members from the information security and fraud prevention departments of the companies have the learning process to prevent ID theft; they have training regarding securing personal and organisational knowledge. However, the staff members working in teams in the non-technical departments do not share their knowledge for ID theft prevention, even though they deal with sensitive information of the customers and the organisation. For example,

staff working in the finance department deal with the financial processes of their companies; teams and groups working in the marketing department deal with the competitive environment and manage the sales data and the competitors' information; teams working in the call centres deal with customer data; and teams working in the non-technical departments require awareness of how to secure the use of the computers, networks and the existing information of customers, products and the organisation.

However, this study found that the online retail industry organisations are not focusing on the awareness of ID theft issues and its protection for the teams working in non-technical departments in the companies. There is no learning process to educate the teams and individuals of non-technical departments to enhance their knowledge sharing for ID theft prevention.

At the moment, staff members from *Company Y* share their knowledge with others outside their department in the company; staff are trusted to share their knowledge with workers from other departments. On the other hand, in the technical departments in *Company X* and *Company Z,* staff share their knowledge within the organisation. Staff working in the technical department in *Company Y* do not share their knowledge with the staff from non-technical departments. The investigation found that online retail organisations are reluctant to share knowledge across the departments within the organisations.

Job rotation plays a vital role in enhancing the knowledge of individuals, teams and departments in the organisations. This research found that only *Company Y* from these researched companies has a policy of job rotation. Individuals are getting the advantage of job rotation to learn new things while working in different departments and the staff working in the department learn from the knowledge and experiences of persons moved into their department. However, *Company Y* is not focusing on the process of knowledge sharing for ID theft prevention in the organisation. None of the researched companies have the policy of job rotation for the sake of enhancing the knowledge of ID theft prevention across the department.

This research found that departments are not sharing the knowledge for ID theft prevention. In fact, the online retail industry organisations do not have a policy of sharing the knowledge for ID theft prevention across departments in the company.

7.4. Research Objective 3: Investigation of existing barriers in knowledge sharing for ID theft prevention in organisations

The present study identified staff unwillingness, lack of individual staff awareness, insufficient learning opportunities, distrust of other staff members, fear of information leakage, insufficient information sourcing opportunities and inefficient ICT infrastructure, lack of leadership support, weak knowledge sharing culture, and no job rotation are the barriers in the process of knowledge sharing for ID theft prevention in online retail organisations. The current study agrees with the findings of the literature (see Section 2.5) that there is a need to remove the existing barriers in the process of knowledge sharing for ID theft prevention in the online retail organisations.

7.5. Research Objective 4: To extend a guiding framework for improving knowledge sharing processes for ID theft prevention inside these organisations

The knowledge sharing framework for an enhanced knowledge sharing process for ID theft prevention in online retail organisations was extended on the basis of the findings of the current research study. Figure 6.3 in Chapter 6 shows the extended framework having important factors known as 'knowledge enablers'. These knowledge enablers are vital for increasing the knowledge sharing process for ID theft prevention in online retail organisations. For example:

KM Infrastructure - a better infrastructure of KM can increase the knowledge of ID theft prevention. It can be used to increase IT skills. Companies need to use their existing tools to share knowledge for ID theft prevention and bring in more knowledge sharing tools to facilitate staff to increase their knowledge.

ICT Know-how and Training - this is for awareness of the information and communication technologies required to secure the usage and distribution of information from the ID thieves. Training and other learning opportunities can be useful for enhancing the knowledge of individuals and teams for ID theft prevention within and outside the departments of the companies.

Job Rotation - the job rotation process plays an important role in increasing the knowledge of staff for ID theft prevention in the companies. It can be useful to provide

awareness to the individuals as well as the teams regarding ID theft issues and how to deal with these issues.

Feedback on Performance Evaluation - according to Shapero (1985), performance evaluation helps in training, continuous learning, boosting robust performance, and consolidating poor performance. Therefore, feedback on performance evaluation is a significant motivator for individuals; it is a means for reception of information needed to improve greater know-how and improvement in their profession (Taylor et al*.,* 2001). Evaluation feedback is important for enhancing the knowledge of individuals in the organisation to prevent ID theft and share its knowledge. Therefore, it is recommended that companies implement a culture of performance evaluation for sharing the knowledge for ID theft prevention within their organisations.

Information Sourcing Opportunities - online retailers are not concentrating on the awareness of ID theft issues and its prevention to their staff. Existing information sources must be used for sharing the knowledge for ID theft prevention inside the companies. Individuals, as well as teams and departments, can avail themselves of these opportunities to enhance knowledge for ID theft identification and its prevention.

Leadership Support - the leadership of all three companies is very supportive and helpful, and the staff members are happy with their management. However, there is the need for an enhanced environment for knowledge sharing for ID theft prevention. Leadership support is needed in the development of an educational environment for enhancing the knowledge for ID theft prevention and sharing knowledge within the organisations so that individuals and teams from different departments can get the advantage of sharing knowledge for ID theft prevention in their companies.

Knowledge sharing culture - this refers to the sharing knowledge among individuals, teams and departments inside the organisation and among different organisations. Organisational culture refers to the shared values, beliefs and performances of persons within organisations (McDermott & O'Dell, 2001). A knowledge sharing culture is one of the main elements to be considered in the organisation for information and knowledge sharing among individuals as well as teams inside the organisation. It is the most important element that needs to be understood in advance before employing any new strategies in the organisation (Syed-Ikhsan & Rowland, 2004). Culture is considered to be a significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM.

According to Stoddart (2001), knowledge sharing can work if the culture of the organisation supports it, and the changes required are developed according to the culture of the organisation.

However, staff members get the advantage of sharing their knowledge for ID theft prevention in information technology and information security departments. Staff members from non-technical departments need to enhance their trust levels, and they need to be educated to enhance their knowledge for ID theft prevention.

7.6. Key Findings of This Study

1. Staff unwillingness, lack of individual staff awareness, insufficient learning opportunities, distrust of other staff members, fear of information leakage, insufficient information sourcing opportunities and inefficient ICT infrastructure, lack of leadership support, weak knowledge sharing culture, and no job rotation are the barriers in the process of knowledge sharing for ID theft prevention in online retail organisations. There is a need to remove the existing barriers in the process of sharing knowledge for ID theft prevention in the online retail organisations.
2. The findings of this study illustrate that knowledge for ID theft prevention is not being shared between individuals or in teams across the departments in the companies. Staff members share the knowledge for ID theft prevention within their own departments. Basic training is being given to newcomers to provide them with the know-how for the systems used and the working activities within the companies.
3. Seminars are arranged on ID theft prevention in one of the researched companies. The online companies need to develop an educational system to enhance the knowledge of employees for effective knowledge sharing process for ID theft prevention. Some policy documents are being disseminated to employees on ID theft prevention which set out awareness of confidential information, but these documents do not describe knowledge sharing process for ID theft prevention. E-mails are used to share their knowledge for their working activities. The companies need to develop a centralised system that can provide information to the employees for ID theft prevention.

4. There is no job rotation in *Company X* and *Company Z*. Employees are learning from their own experience which is time-consuming and exhaustive. On the other hand, *Company Y* has a job rotation process, but it is not being used to enhance the knowledge of staff for ID theft. Job rotation in the organisation is important to enhance the knowledge of individuals, teams and groups. The company needs to rotate the knowledge holders' jobs around different teams across various departments to enhance the knowledge of other staff members on ID theft prevention. Employees trust others within their department and share knowledge with them regarding preventing ID theft. The company needs to enhance the trust level across departments for knowledge sharing for ID theft prevention.
5. This research helps the retail industry enhance the process of knowledge sharing for ID theft prevention within the organisations and provides solutions regarding developing a knowledge sharing culture inside the companies. It also helps the organisations to develop a proper training system to educate their staff to share their knowledge for ID theft prevention. This research also extends a framework for effective knowledge sharing process for ID theft prevention.

7.7. Novel Contribution of This Research

The present study contributed to the existing research and is a practical contribution to online retail organisations.

7.7.1. Theoretical Contributions

The literature review identified that ID theft is a major problem for the online retail sector. Employees working in online retail organisations need to enhance their knowledge of ID theft identification and its prevention. The knowledge of employees can be improved through sharing knowledge for ID theft prevention. Through the process of research refinement, this study could not find any research work done on the investigation of knowledge sharing processes for ID theft prevention in the online retail organisations, resulting in a gap in the area of the research study. It also contributes to existing research by providing new insights into knowledge sharing for identity theft prevention. It has investigated knowledge sharing processes for ID theft prevention within online retail organisations in the UK. The present research studied and analysed ways in which

individual staff members share their knowledge for ID theft prevention with each other, investigated the knowledge sharing processes between teams within and outside their departments in the organisations, and identified existing barriers in knowledge sharing for ID theft prevention in organisations. It also extended a guiding framework proposed by Salleh (2010) in the new context of knowledge sharing processes for ID theft prevention in the retail industry by simplifying the model and combining elements into a more coherent framework. The extended framework is discussed in detail in section 6.5.1.

7.7.2. Contributions in Practice

From the perspective of the practical implications, this study investigated online retail organisations and provided solutions for improved knowledge sharing processes for ID theft prevention. The extended framework can be adopted to enhance the knowledge of individuals and teams within and across departments in the company. The empirical research identifies the barriers to knowledge sharing for ID theft prevention and highlights the weaknesses of knowledge sharing processes in online retail organisations relevant to ID theft prevention. Finally, this study also provides managers with useful guidelines for developing appropriate knowledge sharing processes for ID theft prevention in the organisations, and to educate staff for effective knowledge sharing.

7.8. Limitations and Recommendations for Future Work on This Research Study

The limitations of this study provide pathways for future research.

1. The findings of this research study are only based on three online retail companies in the UK. In the results, the investigator recognises that the outcomes may not be illustrative of the whole populace. Therefore, more research is required using an empirical method and focusing on larger numbers. The significance of the outcomes should not be passed over, however, as it was the first study addressing a practical online retail industry problem.
2. This study is limited to the use of the case study approach, the limited number of interviews conducted, the number of internal documents of the researched companies, and the non-availability of existing literature and data from the organisations because of confidentiality concerns. Therefore, future research would

be strengthened by using quantitative research methods for testing the validity of the research outcomes across the whole online retail sector.

3. The researcher carried out this study in the UK's online retail sector, and therefore queries might be raised as to the applicability of the findings outside the UK. Future research is thus recommended for the generalisation of this study work for other countries.
4. It will also be vital to find out the impact on the awareness of individuals and teams by implementing the enhanced knowledge sharing processes for ID theft prevention in online retail organisations; it might impact on the approach of staff to adopt the knowledge sharing process. Therefore, the findings of this study must be implemented to carry out the experiment in online retail industry organisations.
5. The outcomes of this study change the knowledge sharing culture of the organisation. Therefore, further research is required to investigate the behavioural changes of employees caused by implementing the outcomes of this study in online retail organisations.
6. The investigation of managerial practices for ID theft prevention in the organisations.
7. The impact of ID theft prevention knowledge sharing on employees in an organisation.
8. Evaluation of knowledge sharing tools to prevent ID theft in an organisation.

References

Abdullah, Shah, M. H., & Ahmed, W. (2016). Identity theft prevention in online retail organisations: a knowledge sharing framework. *The Business & Management Review,* 8(1), 71-85.

Abecassis-Moedas, C., & Rodrigues Pereira, J. (2016). External design for reputation, perspective and exposure. *Creativity and Innovation Management,* 25(3), 396–407

Abou-Zeid, E. (2005). A culturally aware model of inter-organizational knowledge transfer. *Knowledge Management Research & Practice,* 3(3), 146-155.

Aga, D. A., Noorderhaven, N., & Vallejo, B. (2016). Transformational leadership and project success: The mediating role of team-building. *International Journal of Project Management,* 34(5), 806-818.

Agrawal, A. K. (2001). University-to-industry knowledge transfer: Literature review and unanswered questions. *International Journal of Management Reviews,* 3(4), 285-302.

Agrawal, S., & Budetti, P. (2012). Physician medical identity theft. *The Journal of the American Medical Association,* 307(5), 459-460.

Aïmeur, E., & Schonfeld, D. (2011). The ultimate invasion of privacy: Identity theft. *Ninth Annual International Conference on Privacy, Security and Trust,* Concordia University Montreal, QC, Canada, 24-31, IEEE.

Al-Ghassani, A. M., Kamara, J. M., Anumba, C. J., & Carrillo, P. M. (2004). An innovative approach to identifying knowledge management problems. *Engineering, Construction and Architectural Management,* 11(5), 349-357.

Al Sabbagh, B., Ameen, M., Watterstam, T., & Kowalski, S. (2012). A prototype for HI(2) ping information security culture and awareness training. *International Conference on e-Learning and e-Technologies in Education,* Technical University of Lodz, Poland, 32-36, IEEE.

Alamahamid, S., McAdam, A., & Kalaldeh, T. (2010). The relationship among organizational knowledge sharing practices, employees learning commitments, employees adaptability and employees job satisfaction: An empirical investigation of the listed manufacturing companies in Jordan. *International Journal of Information and Knowledge Management,* 5, 327-355.

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly,* 25(1), 107-136.

Alder, G. S., & Ambrose, M. L. (2005). An examination of the effect of computerized performance monitoring feedback on monitoring fairness, performance, and satisfaction. *Organizational Behaviour and Human Decision Processes,* 97(2), 161-177.

Al-Ghassani, A. M., Anumba, C. J., Carrillo, P. M., & Robinson, H. S. (2005). Tools and techniques for knowledge management. In Carrillo, P. M., Egbu, C. O., & Anumba, C. J. (Eds.), *Knowledge Management in Construction* (pp. 83-102). Oxford: Blackwell Publishing Ltd.

Al-Ghassani, A. M., Carrillo, P. M., Anumba, C. J., & Robinson, H. S. (2001). Software requirements for knowledge management in construction organisations. *Proceedings of the 17th Annual ARCOM Conference,* University of Salford, Manchester, 199-206.

Allen, T. J. (1977). *Managing the flow of technology: Technology transfer and the dissemination of technological information within the R and D organization.* UK: Massachusetts Institute of Technology, Cambridge, MA.

Allison, S. F. H., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice,* 33(1), 19-29.

Allred, B. B. (2001). Enabling knowledge creation: How to unlock the mystery of tacit knowledge and release the power of innovation. *The Academy of Management Executive,* 15(1), 161-162.

Alvarez, I., Zamanillo, I., & Cilleruelo, E. (2016). Have information technologies evolved towards accommodation of knowledge management needs in Basque SMEs? *Technology in Society,* 46, 126-131.

Amin, A., Hassan, M. F. B., & Ariffin, M. B. M. (2010). Framework of intrinsic and extrinsic motivators of knowledge sharing: A case of training institutes of an oil and gas company in Malaysia. *Proceedings of International Symposium in Information Technology (ITSim),* Kuala Lumpur, 3, 1428-1432, IEEE.

Andersen, S. N., & Broberg, O. (2016). A framework of knowledge creation processes in participatory simulation of hospital work systems. *Ergonomics,* (just-accepted), 1-39.

Andrews, K. M., & Delahaye, B. L. (2000). Influences on knowledge processes in organizational learning: The psychosocial filter. *Journal of Management Studies,* 37(6), 797-810.

Anumba, C. J., Egbu, C., & Carrillo, P. (2008). *Knowledge management in construction,* (Eds.). Oxford: John Wiley & Sons.

Arachchilage, N. A. G., Love, S., & Scott, M. (2012). Designing a mobile game to teach conceptual knowledge of avoiding "Phishing attacks". *International Journal for e-Learning Security,* 2(2), 127-132.

Ardichvili, A., Page, V., & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. *Journal of Knowledge Management,* 7(1), 64-77.

Argote, L. (2012). *Organizational learning: Creating, retaining and transferring knowledge* (2nd ed.), London: Springer Science & Business Media.

Argote, L., & Ingram, P. (2000). Knowledge transfer: A basis for competitive advantage in firms. *Organizational Behavior and Human Decision Processes,* 82(1), 150-169.

Argote, L., McEvily, B., & Reagans, R. (2003). Managing knowledge in organizations: An integrative framework and review of emerging themes. *Management Science,* 49(4), 571-582.

Bălău, N., & Utz, S. (2016). Exposing information sharing as strategic behaviour: Power as responsibility and "Trust" buttons. *Journal of Applied Social Psychology.*

Barnes, P. (2001). A primer on knowledge management. *Student Accountant (ACCA, UK), 2001* (August), 30-36.

Bass, B. M., & Stogdill, R. M. (1990). *Bass & stogdill's handbook of leadership: Theory, research, and managerial applications,* (3rd ed.). London: Simon and Schuster.

Becker, H. S. (2008). *Tricks of the trade: How to think about your research while you're doing it.* London: University of Chicago Press.

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security,* 13(3), 189-202.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly,* 11(3), 369-386.

Bentz, V. M., & Shapiro, J. J. (1998). *Mindful inquiry in social research*. London: Sage Publications.

Bernard, H. R., & Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches* (2nd ed.). London: Sage.

Bhaskar, R. (1978). *A realist theory of science*. Sussex: Harvester Press.

Bhatt, G., Emdad, A., Roberts, N., & Grover, V. (2010). Building and leveraging information in dynamic environments: The role of IT infrastructure flexibility as enabler of organizational responsiveness and competitive advantage. *Information & Management,* 47(7), 341-349.

Bhatt, G. D. (2001). Knowledge management in organizations: Examining the interaction between technologies, techniques, and people. *Journal of Knowledge Management,* 5(1), 68-75.

Bhatt, G. D. (2002). Management strategies for individual knowledge and organizational knowledge. *Journal of Knowledge Management,* 6(1), 31-39.

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: Automated identity theft attacks on social networks. *Proceedings of the 18th International Conference on World Wide Web,* New York, 551-560.

Bindra, G. S., Shrivastava, D., & Seth, R. (2012). With attackers wearing many hats, prevent your "Identity theft". *6th International Conference on Application of Information and Communication Technologies,* Georgia, Tbilisi, 1-5, IEEE.

Blaikie, N. (1993). *Approaches to social enquiry: Advancing knowledge*. Cambridge, UK: Polity Press.

Blaikie, N. (2007). *Approaches to social enquiry: Advancing knowledge,* (2nd ed.). Cambridge: Polity.

Bock, G., & Kim, Y. (2001). Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing. *Proceedings of Pacific Asia Conference on Information Systems,* Seoul, Korea, 1112-1125.

Boerner, S., Eisenbeiss, S. A., & Griesser, D. (2007). Follower behaviour and organizational performance: The impact of transformational leaders. *Journal of Leadership & Organizational Studies,* 13(3), 15-26.

Bollinger, A. S., & Smith, R. D. (2001). Managing organizational knowledge as a strategic asset. *Journal of Knowledge Management,* 5(1), 8-18.

Bos, N., Olson, J., Gergle, D., Olson, G., & Wright, Z. (2002). Effects of four computer-mediated communications channels on trust development. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* Minneapolis, Minnesota.

Bose, I., & Leung, A. C. M. (2013). The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems,* 55(3), 753-763.

Boxall, P. (1996). The strategic HRM debate and the resource-based view of the firm. *Human Resource Management Journal,* 6(3), 59-75.

Bradford, T., & Cundiff, B. (2006). Payments fraud: Consumer considerations. *Payments System Research Briefing,* (May), 1-5

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology,* 3(2), 77-101.

Brown, J. W., & Utterback, J. M. (1985). Uncertainty and technical communication patterns. *Management Science,* 31(3), 301-311.

Brown, A. D., & Starkey, K. (1994). The effect of organizational culture on communication and information. *Journal of Management studies*, 31(6), 807-828.

Bryman, A. (1984). The debate about quantitative and qualitative research: A question of method or epistemology? *British Journal of Sociology,* 35(1), 75-92.

Bryman, A. (2013). *Doing research in organizations,* London, Routledge.

Bryman, A., & Bell, E. (2015). *Business research methods* (4th ed.). Oxford: Oxford university press.

Bryman, A. (2015). *Social research methods* (5th ed.) Oxford University Press.

Bush, D. (2016). How data breaches lead to fraud. *Network Security,* 2016(7), 11-13.

Cabrera, A., & Cabrera, E. F. (2002). Knowledge-sharing dilemmas. *Organization Studies,* 23(5), 687-710.

Carolan, C. M., Forbat, L., & Smith, A. (2016). Developing the DESCARTE model: The design of case study research in health care. *Qualitative Health Research,* 26(5), 626-639.

Carrillo, P. M., Robinson, H., Al-Ghassani, A., & Anumba, C. J. (2004). Knowledge management in UK construction: Strategies, resources and barriers.

Carter, S. M., & Little, M. (2007). Justifying knowledge, justifying method, taking action: Epistemologies, methodologies, and methods in qualitative research. *Qualitative Health Research,* 17(10), 1316-1328.

Cavaye, A. L. M. (1996). Case study research: A multi-faceted research approach for IS. *Information Systems Journal,* 6(3), 227-242.

Chang, H. H., & Chuang, S. (2011). Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator. *Information & Management,* 48(1), 9-18.

Charband, Y., & Navimipour, N. J. (2016). Online knowledge sharing mechanisms: A systematic review of the state of the art literature and recommendations for future research. *Information Systems Frontiers,* 1-21.

Charmaz, K. (2000). Grounded Theory: objectivist and constructivist methods in Norman K. Denzin and Yvonne S. Lincoln (eds.) Handbook of Qualitative Research. Thousand Oaks, CA: Sage

Chen, G. L., Ling, W. Y., Yang, S. C., Tang, S. M., & Wu, W. C. (2011). Explicit knowledge and tacit knowledge sharing. *International Conference on Management and Service Science,* 1-4, Wuhan.

Chen, S., Duan, Y., Edwards, J. S., & Lehaney, B. (2006). Toward understanding inter-organizational knowledge transfer needs in SMEs: Insight from a UK investigation. *Journal of Knowledge Management,* 10(3), 6-23.

Chen, B. -., Kifer, D., LeFevre, K., & Machanavajjhala, A. (2009). Privacy-preserving data publishing. *Foundations and Trends in Databases,* 2(1-2), 1-167.

Cho, Y., & Lee, S. (2016). Detection and response of identity theft within a company utilizing location information. *International Conference on Platform Technology and Service,* Jeju, 1-5.

Chohan, R., Shah, M., Larson, M., & Welch, M. (2014). Overcoming trust barriers: Evaluating inter-organisational knowledge sharing in UK online retail sector. *15th European Conference on Knowledge Management*, Santarem, Portugal, 3, 1156-1163, Academic Conferences International Ltd.

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals in organizational knowledge sharing. *Information & Management,* 45(7), 458-465.

Chuang, C., Jackson, S. E., & Jiang, Y. (2016). Can knowledge-intensive teamwork be managed? Examining the roles of HRM systems, leadership, and tacit knowledge. *Journal of Management,* 42(2), 524-554.

CIFAS. (2012). FRAUDSCAPE depicting the UK's fraud landscape. Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External%20-%2000%20Fraudscape%202012.pdf

CIFAS. (2013). FRAUDSCAPE depicting the UK's fraud landscape. Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External-Fraudscape_2013_CIFAS.pdf

CIFAS. (2016). FRAUDSCAPE. Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/160706_cifas_fraudscape_ONLINE.pdf

CIFAS. (2017). FRAUDSCAPE 2017, External and internal fraud threats – essential reading for fraud and financial crime strategists. Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External-Fraudscape%20report%202017.pdf

Cobo, C. (2013). Skills for innovation: Envisioning an education that prepares for the changing world. *Curriculum Journal,* 24(1), 67-85.

Cohen, S. G., & Bailey, D. E. (1997). What makes teams work: Group effectiveness research from the shop floor to the executive suite. *Journal of Management,* 23(3), 239-290.

Cong, X., & Pandya, K. V. (2003). Issues of knowledge management in the public sector. *Electronic Journal of Knowledge Management,* 1(2), 25-33.

Conrad, E., Misenar, S., & Feldman, J. (2012). *CISSP Study Guide.* Access Online via Elsevier.

Cooney, R. (2004). Empowered self-management and the design of work teams. *Personnel Review,* 33(6), 677-692.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed). London: Sage.

Creswell, J. W., & Clark, V. L. P. (2007). Designing and conducting mixed methods research. *Australian and New Zealand Journal of Public Health,* 31(4), 388-389

Cross, R., Parker, A., Prusak, L., & Borgatti, S. P. (2001). Knowing what we know: Supporting knowledge creation and sharing in social networks. *Organizational Dynamics,* 30(2), 100-120.

CRR. (2016). Online retailing: Britain, Europe, US and Canada 2016. Retrieved from http://www.retailresearch.org/onlineretailing.php

Cui Guang-Bin, Li Yi-Jun, & Dong Liang. (2010). Study on the incentive mechanism model of tacit knowledge sharing. *2nd International Conference on Information Management and Engineering,* Chengdu, 486-490, IEEE.

Cummings, J. L., & Teng, B. (2003). Transferring R&D knowledge: The key factors affecting knowledge transfer success. *Journal of Engineering and Technology Management,* 20(1), 39-68.

Dainty, A., Qin, J., & Carrillo, P. (2005). HRM strategies for promoting knowledge sharing within construction project organisations. In: Kazi, A.S., (Eds.), *Knowledge Management in the Construction Industry: A Socio-Technical Perspective.* (pp. 18-33). London: Idea Group Publishing.

Daneshgar, F. (2001). Maintaining collaborative process awareness as a mechanism for knowledge sharing. *2nd European Conference on Knowledge Management,* Bled, Slovenia.

Davenport, T. H., Jarvenpaa, S. L., & Beers, M. C. (1996). Improving knowledge work processes. *MIT Sloan Management Review,* 37(4), 53.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know.* Boston: Harvard Business Press.

David, S. (Ed.). (2004). *Qualitative research theory method and practice* (2nd ed.). London: Sage.

De Grip, A., & Sauermann, J. (2013). The effect of training on productivity: The transfer of on-the-job training from the perspective of economics. *Educational Research Review,* 8(0), 28-36.

Dede, C. (2010). Comparing frameworks for 21st century skills. In: Bellanca, J., & Brandt, R., (Eds.), *21st Century Skills: Rethinking how Students Learn.* (pp. 51-76). US: Solution Trees Press.

Delanty, G. (2005). *Social science: Philosophical and methodological foundations* (2nd ed.). Berkshire, England: Open University Press.

Denzin, N. K., & Lincoln, Y. (2000). *Handbook of Qualitative Research* (2nd ed.). London: Sage.

Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE Handbook of Qualitative Research* (4th ed.). London: Sage.

Desouza, K. C. (2006). Knowledge security: An interesting research space. *Journal of Information Science and Technology,* 3(1), 1-7.

Desouza, K. C., & Vanapalli, G. K. (2005). Securing knowledge in organizations: Lessons from the defense and intelligence sectors. *International Journal of Information Management,* 25(1), 85-98.

Disterer, G. (2001). Individual and social barriers to knowledge transfer. *Proceedings of 34th Annual Hawaii International Conference on System Sciences,* Maui, HI, USA, 1-7.

Dobson, P. J. (2001). The philosophy of critical realism—an opportunity for information systems research. *Information Systems Frontiers, 3*(2), 199-210.

Donate, M. J., & Guadamillas, F. (2015). An empirical study on the relationships between knowledge management, knowledge-oriented human resource practices and innovation. *Knowledge Management Research & Practice,* 13(2), 134-148.

Duan, Y., Xu, X., & Fu, Z. (2006). Understanding transnational knowledge transfer. *Proceedings of the 7th European Conference on Knowledge Management,* Budapest, Hungary*,* 126-135.

Duan, Y., Nie, W., & Coakes, E. (2010). Identifying key factors affecting transnational knowledge transfer. *Information & Management,* 47(7–8), 356-363.

Duke, K. (2002). Getting beyond the 'Official line': Reflections on dilemmas of access, knowledge and power in researching policy networks. *Journal of Social Policy,* 31(1), 39-59.

Dymock, D., & McCarthy, C. (2006). Towards a learning organization? Employee perceptions. *The Learning Organization,* 13(5), 525-537.

Egbu, C. (2000). The role of IT in strategic knowledge management and its potential in the construction industry. *UK National Conference on Objects and Integration for Architecture, Engineering, and Construction,* BRE, Watford, UK.

Egbu, C. O. (2004). Managing knowledge and intellectual capital for improved organizational innovations in the construction industry: An examination of critical success factors. *Engineering, Construction and Architectural Management,* 11(5), 301-315.

Eisenstein, E. M. (2008). Identity theft: An exploratory study with implications for marketers. *Journal of Business Research,* 61(11), 1160-1172.

Eriksson, T., & Ortega, J. (2006). The adoption of job rotation: Testing the theories. *Industrial & Labor Relations Review,* 59(4), 653-666.

Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behaviour. *Information Systems Frontiers,* 15(1), 5-15.

Faraj, S., & Sproull, L. (2000). Coordinating expertise in software development teams. *Management Science,* 46(12), 1554-1568.

Feledi, D., & Fenz, S. (2012). Challenges of web-based information security knowledge sharing. *Seventh International Conference on Availability, Reliability and Security,* Prague, 514-521, IEEE.

Fennelly, L. J. (2012). *Handbook of Loss Prevention and Crime Prevention* (5th ed.). London: Elsevier Inc.

Fernie, S., Green, S. D., Weller, S. J., & Newcombe, R. (2003). Knowledge sharing: Context, confusion and controversy. *International Journal of Project Management,* 21(3), 177-187.

Fielding, N., & Thomas, H. (2015). Qualitative interviewing. In: Gilbert, N., & Stoneman, P. (Eds.). *Researching Social Life* (4th ed). London: Sage.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions, *IEEE Communications Surveys & Tutorials,* 16(4), 2019 - 2036

Fremeth, A. R., Holburn, G. L., & Richter, B. K. (2016). Bridging qualitative and quantitative methods in organizational research: Applications of synthetic control methodology in the US automobile industry. *Organization Science,* 27(2), 462-482.

Gabelica, C., Bossche, P. V. d., Segers, M., & Gijselaers, W. (2012). Feedback, a powerful lever in teams: A review. *Educational Research Review,* 7(2), 123-144.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research,* 16(2), 186-208.

Gillham, B. (2000). *Case study research methods.* UK: Continuum International Publishing Group.

Gillian Ragsdell, D., Corfield, A., & Paton, R. (2016). Investigating knowledge management: Can KM really change organisational culture? *Journal of Knowledge Management,* 20(1), 88-103.

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The Discovery of Grounded Theory; Strategies for Qualitative Research. *Nursing Research*, 17(4), 364

Goh, S. C. (2002). Managing effective knowledge transfer: An integrative framework and some practice implications. *Journal of Knowledge Management,* 6(1), 23-30.

Gomm, R., Hammersley, M., & Foster, P. (2000). *Case study method: Key issues, key texts.* London: Sage.

Gordon, G. R., Rebovich, D. J., Choo, K., & Gordon, J. (2007). Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement. *Center for Identity Management and Information Protection*, Utica College, NY. Retrieved from: https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=242217

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy,* 22(6), 461-485.

Goulding, C. (2002). *Grounded theory: A practical guide for management, business and market researchers*. London: Sage.

Gould-Williams, J. S. (2016). Managers' motives for investing in HR practices and their implications for public service motivation: a theoretical perspective. *International Journal of Manpower*, 37(5), 764-776.

Grant, R. M., & Baden-Fuller, C. (2004). A knowledge accessing theory of strategic alliances. *Journal of Management Studies,* 41(1), 61-84.

Graves, J. T., Acquisti, A., & Christin, N. (2016). Big data and bad data: On the sensitivity of security policy to imperfect information. *The University of Chicago Law Review,* 83(1)*,* 117-137.

Gray, J., & Laidlaw, H. (2002). Part-time employment and communication satisfaction in an Australian retail organisation. *Employee Relations,* 24(2), 211-228.

Gregg, R. S. (2013). Systems and Methods for Reducing Medical Claims Fraud. *U.S. Patent Application No. 13/296,159*.

Grover, A., Berghel, H., & Cobb, D. (2011). The state of the art in identity theft. In Marvin V. Zelkowitz (Eds.), *Advances in Computers* (pp. 1-50). London: Elsevier Inc.

Guang-bin, C., Liang, D., Yi-Jun, L., & Tao, G. (2010). Study on multi-levels incentive mechanism model for tacit knowledge sharing in enterprise. *International Conference on E-Business and E-Government,* Guangzhou, 1948-1951.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research, Morse, J. M., Denzin, N. K., & Lincoln, Y. S. (edits). *Handbook of Qualitative Research.* London: Sage.

Guo, K. H. (2010). Knowledge for managing information systems security: Review and future research directions. In Alkhalifa, E. (Ed.), *E-Strategies for Resource Management Systems: Planning and Implementation* (pp. 266-288). NY: Business Science Reference.

Gupta, A. K., & Govindarajan, V. (2000). Knowledge management's social dimension: Lessons from nucor steel. *MIT Sloan Management Review,* 42(1), 71.

Gupta, B., Iyer, L. S., & Aronson, J. E. (2000). Knowledge management: Practices and challenges. *Industrial Management & Data Systems,* 100(1), 17-21.

Haas, M. R., & Hansen, M. T. (2007). Different knowledge, different benefits: Toward a productivity perspective on knowledge sharing in organizations. *Strategic Management Journal,* 28(11), 1133-1153.

Hackman, J. (1987). The design of work teams. In Lorsch, J. W. (Ed.), *Handbook of Organizational Behavior* (pp. 315-342). New Jersey: Prentice Hall

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics,* 133(1), 111-123.

Hakim, C. (2000). *Research design: Successful designs for social and economic research* (2nd ed.). London: Psychology Press.

Hancock, D. R., & Algozzine, B. (2015). *Doing case study research: A practical guide for beginning researchers.* New York: Teachers College Press.

Hansen, M. T. (2002). Knowledge networks: Explaining effective knowledge sharing in multiunit companies. *Organization Science,* 13(3), 232-248.

Harteis, C., Bauer, J., & Gruber, H. (2008). The culture of learning from mistakes: How employees handle mistakes in everyday work. *International Journal of Educational Research,* 47(4), 223-231.

Hartley, J. (2004). Case study research. In Cassell, C., & Symon, G. (Eds.). *Essential Guide to Qualitative Methods in Organizational Research* (pp. 323-333). London: Sage.

Hashim, K. F., & Tan, F. B. (2015). The mediating role of trust and commitment on members' continuous knowledge sharing intention: A commitment-trust theory perspective. *International Journal of Information Management,* 35(2), 145-151.

He, W., & Wei, K. (2009). What drives continued knowledge sharing? An investigation of knowledge-contribution and-seeking beliefs. *Decision Support Systems,* 46(4), 826-838.

Health and Human Services. (2012). Health information privacy. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/indexnumbers.html

Henttonen, K., Kianto, A., & Ritala, P. (2016). Knowledge sharing and individual work performance: An empirical study of a public sector organisation. *Journal of Knowledge Management,* 20(4), 749-768.

Hessler, R. M. (1992). *Social research methods,* Thomson Learning.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing,* 30, 1-19.

Hislop, D. (2002). Managing knowledge and the problem of commitment. *The Third European Conference on Organizational Knowledge, Learning, and Capabilities,* Astir Palace, Athens, 5-6.

Hoar, S. B. (2001). Identity theft: The crime of the new millennium. *Oregon Law Review,* 80, 1423- 1447.

Holsapple, C. (2013). *Handbook on knowledge management 1: Knowledge matters*. Heidelberg, USA, Springer Science & Business Media.

Holt, D. (2000). The measurement of readiness for change: A review of instruments and suggestions for future research. *Annual Meeting of the Academy of Management.* Toronto, Canada.

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older internet users. *Psychology, Crime & Law,* 21(7), 681-698.

Holtshouse, D., Borghoff, U. M., & Pareschi, R. (2013). *Information technology for knowledge management* (Eds.). New York: Springer Science & Business Media.

Homans, G. C. (1958). Social behaviour as exchange. *American Journal of Sociology,* 63(6), 597-606.

Horibe, F. (1999). *Managing knowledge workers: New skills and attitudes to unlock the intellectual capital in your organization.* New York: John Wiley & Sons.

Hortovanyi, L., & Ferincz, A. (2015). The impact of ICT on learning on-the-job. *The Learning Organization,* 22(1), 2-13.

Hsu, I. (2006). Enhancing employee tendencies to share knowledge - Case studies of nine companies in Taiwan. *International Journal of Information Management,* 26(4), 326-338.

Hsu, M., Ju, T. L., Yen, C., & Chang, C. (2007). Knowledge sharing behaviour in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies,* 65(2), 153-169.

Huang, H., Liao, M., & Thou, Z. (2005). An empirical study on relativity among job rotation, job satisfaction and organization commitment. *Journal of Human Resource Management,* 5(4), 107-129.

Huang, K. (2014). Knowledge sharing in a Third-Party-Governed health and human services network. *Public Administration Review,* 74(5), 587-598.

Huang, Q., Davison, R. M., & Gu, J. (2011). The impact of trust, guanxi orientation and face on the intention of Chinese employees and managers to engage in peer-to-peer tacit and explicit knowledge sharing. *Information Systems Journal,* 21(6), 557-577.

Huang, S., & Pan, Y. (2014). Ergonomic job rotation strategy based on an automated RGB-D anthropometric measuring system. *Journal of Manufacturing Systems,* 33(4), 699-710.

Hughes, J. A., & Sharrock, W. W. (1997). The philosophy of social research.

Hülsheger, U. R., Anderson, N., & Salgado, J. F. (2009). Team-level predictors of innovation at work: A comprehensive meta-analysis spanning three decades of research. *Journal of Applied Psychology,* 94(5), 1128.

Hussain, F., Lucas, C., & Ali, M. (2004). Managing knowledge effectively. *Journal of Knowledge Management Practice,* 5(1), 1-12.

Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers,* 15(1), 1-4.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizations: Adoption and impact of technology. *MIS Quarterly,* 19(4), 465-485.

I-Ching Hsu, Lee Jang Yang, & Der-Chen Huang. (2011). Knowledge sharing platform for project team based on web feeds. *International Conference on Uncertainty Reasoning and Knowledge Engineering,* Bali*,* 67-70, IEEE.

Ilvonen, I., Alanne, A., Helander, N., & Vayrynen, H. (2016). Knowledge sharing and knowledge security in finnish companies. *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, 4021-4030, IEEE.

Ingram, D. M. (2006). How to minimize your risk of identity theft. *Optometry - Journal of the American Optometric Association,* 77(6), 312-314.

Ipe, M. (2003). Knowledge sharing in organizations: A conceptual framework. *Human Resource Development Review,* 2(4), 337-359.

Iqbal, S., Toulson, P., & Tweed, D. (2015). Employees as performers in knowledge intensive firms: Role of knowledge sharing. *International Journal of Manpower,* 36(7), 1072-1094.

Islam, M. Z., Hasan, I., & Zain, A. Y. M. (2012). The impact of organizational culture and structure on knowledge sharing. *Proceedings of USM-AUT International Conference Sustainable Economic Development: Policies and Strategies,* Penang, Malaysia*,* 167, 285-298.

Ismail, M. B., & Yusof, Z. M. (2010). The impact of individual factors on knowledge sharing quality. *Journal of Organizational Knowledge Management,* 13, 1-12

Ives, W., Torrey, B., & Gordon, C. (1997). Knowledge management: an emerging discipline with a long history. *Journal of Knowledge Management*, 1(4), 269-274.

Jalaldeen, M., Razi, M., Karim, A., Shariza, N., & Mohamed, N. (2009). Organizational readiness and its contributing factors to adopt km processes: A conceptual model. *Communications of the IBIMA,* 8(17), 128-136.

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology,* 35(5), 368-379.

Jashapara, A. (2004). *Knowledge management: An integral approach.* Essex: Pearson Education Ltd.

Jayasingam, S., Govindasamy, M., & Singh, S. K. G. (2016). Instilling affective commitment: Insights on what makes knowledge workers want to stay. *Management Research Review,* 39(3), 266-288.

Jin, L., Takabi, H., & Joshi, J. B. (2011). Towards active detection of identity clone attacks on online social networks. *Proceedings of the First ACM Conference on Data and Application Security and Privacy,* New York.

Joe Laidler, K., Joe Laidler, K., Lee, M., & Lee, M. (2016). Thirty years of criminology at HKU: Themes and trends in crime and its control. *Social Transformations in Chinese Societies,* 12(1), 21-36.

Joffe, H., & Yardley, L. (2004). 4. Content and thematic analysis. In: David F. Marks and Lucy Yardley (Eds.), *Research methods for clinical health and psychology* (pp. 56-68). London: Sage.

Jones, G. R., & George, J. M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of Management Review,* 23(3), 531-546.

Jonsson, A., & Kalling, T. (2007). Challenges to knowledge sharing across national and intra-organizational boundaries: Case studies of IKEA and SCA packaging. *Knowledge Management Research & Practice,* 5(3), 161-172.

Jung-Chi Pai. (2006). An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP). *Management Decision,* 44(1), 105-122.

Kalid, K. S., & Mahmood, A. K. (2011). The development of a knowledge management storytelling process framework for the purpose of transferring knowledge. *International Conference on Research and Innovation in Information Systems,* Kuala Lumpur.

Kampkötter, P., Harbring, C., & Sliwka, D. (2016). Job rotation and employee performance–evidence from a longitudinal study in the financial services industry. *The International Journal of Human Resource Management*, 1-27.

Kane, A. A., Argote, L., & Levine, J. M. (2005). Knowledge transfer between groups via personnel rotation: Effects of social identity and knowledge quality. *Organizational Behavior and Human Decision Processes,* 96(1), 56-71.

Kelle, U. (2006). Combining qualitative and quantitative methods in research practice: Purposes and advantages. *Qualitative Research in Psychology, 3*(4), 293-311.

Khan, F., ur Rehman, A., Arif, M., Aftab, M., & Jadoon, B. K. (2016). A survey of communication technologies for smart grid connectivity. *International Conference on Computing, Electronic and Electrical Engineering (ICE Cube),* Quetta, 256-261.

Kikoski, C. K., & Kikoski, J. F. (2004). *The inquiring organization: Tacit knowledge, conversation, and knowledge creation: Skills for 21st-century organizations.* Westport: Greenwood Publishing Group.

Kim, S., & Lee, H. (2004, May). Organizational factors affecting knowledge sharing capabilities in e-government: An empirical study. *IFIP International Working Conference on Knowledge Management in Electronic Government,* Berlin Heidelberg, 281-293, Springer.

Kim, S., & Lee, H. (2006). The impact of organizational context and information technology on employee knowledge-sharing capabilities. *Public Administration Review,* 66(3), 370-385.

Kolaczek, G. (2009). An approach to identity theft detection using social network analysis. *First Asian Conference on Intelligent Information and Database Systems,* Dong Hoi, 78-81.

Koops, B., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. *Datenschutz Und Datensicherheit-DuD,* 30(9), 553-556.

Kozlowski, A., Searcy, C., & Bardecki, M. (2016). Innovation for a sustainable fashion industry: A design focused approach toward the development of new business models. In: Muthu, S. S., & Gardetti, M. A. (Eds.), *Green fashion* (pp. 151-169). Singapore: Springer.

Kumar, P., & Kumar, R. (2016). Cyber security's significance in health information technology (HIT). *International Journal of Advanced Studies in Computers, Science and Engineering,* 5(2), 8.

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems,* 52(2), 353-363.

Lai, J., Lui, S. S., & Tsang, E. W. (2016). Intrafirm knowledge transfer and employee innovative behaviour: The role of total and balanced knowledge flows. *Journal of Product Innovation Management,* 33(1), 90-103.

Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems,* 52(2), 353-363.

Lam, A., & Jean-Paul Lambermont-Ford. (2010). Knowledge sharing in organisational contexts: A motivation-based perspective. *Journal of Knowledge Management,* 14(1), 51-66.

Lam, H. (2016). Social media dilemmas in the employment context. *Employee Relations,* 38(3), 420-437.

Lather, P. (1992). Critical frames in educational research: Feminist and post-structural perspectives. *Theory into Practice,* 31(2), 87-99.

Lee, C. K., & Al-Hawamdeh, S. (2002). Factors impacting knowledge sharing. *Journal of Information & Knowledge Management,* 1(01), 49-56.

Lee, H., & Choi, B. (2003). Knowledge management enablers, processes, and organizational performance: An integrative view and empirical examination. *Journal of Management Information Systems,* 20(1), 179-228.

Lee, M. K., Cheung, C. M., Lim, K. H., & Ling Sia, C. (2006). Understanding customer knowledge sharing in web-based discussion boards: An exploratory study. *Internet Research,* 16(3), 289-303.

Lee, P., Gillespie, N., Mann, L., & Wearing, A. (2010). Leadership and trust: Their effect on knowledge sharing and team performance. *Management Learning,* 1-9, Sage Journals.

Lee, C. K., & Al-Hawamdeh, S. (2002). Factors impacting knowledge sharing. *Journal of Information & Knowledge Management,* 01(01), 49-56.

Letmathe, P., Schweitzer, M., & Zielinski, M. (2012). How to learn new tasks: Shop floor performance effects of knowledge transfer and performance feedback. *Journal of Operations Management,* 30(3), 221-236.

Leyer, M., & Claus, N. (2013). Toward an agile knowledge connection of employees with regard to business processes. *46th Hawaii International Conference on System Sciences,* Wailea, HI, USA, 3436-3445, IEEE.

Liebowitz, J. (1999). *Knowledge management handbook*. London: CRC press.

Liu Lihua, Xu Jichao, & Yang Ping. (2010). Notice of retraction the impact of shared product knowledge and receivers' expertise on the e-commerce consumer purchasing decision. *International Conference on Advanced Management Science,* Chengdu, 744-747, IEEE.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems,* 52(1), 95-107.

Lovell, S. A., & Rosenberg, M. W. (2016). Community capacity building through qualitative methodologies. In Fenton, N. E., & Baxter, J. (Eds.), *Practicing Qualitative Methods in Health Geographies,* London: Routledge.

Lu, L., Leung, K., & Koch, P. T. (2006). Managerial knowledge sharing: The role of individual, interpersonal, and organizational factors. *Management and Organization Review,* 2(1), 15-41.

Luen, T. W., & Al-Hawamdeh, S. (2001). Knowledge management in the public sector: Principles and practices in police work. *Journal of Information Science,* 27(5), 311-318.

Luu, T. T. (2013). Leading to learning and competitive intelligence. *The Learning Organization,* 20(3), 216-239.

MacNeil, C. M. (2003). Line managers: Facilitators of knowledge sharing in teams. *Employee Relations,* 25(3), 294-307.

Madiwalar, M. B. (2016). Privacy rights and data protection in cyber space with special reference to E-commerce. *Global Journal for Research Analysis,* 4(12), 319-321

Majewski, G., Usoro, A., & Khan, I. (2011). Knowledge sharing in immersive virtual communities of practice. *VINE Journal of Information and Knowledge Management Systems,* 41(1), 41-62.

Mansourov, N., & Campara, D. (2011). *System assurance Beyond Detecting Vulnerabilities*. London, Morgan Kaufmann Publishers.

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: The practice perspective. *The Journal of Strategic Information Systems,* 21(1), 18-30.

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research* (3rd ed.). London: Sage.

Marshall, A. M., & Tompsett, B. C. (2005). Identity theft in an online world. *Computer Law and Security Report,* 21(2), 128-137.

Martin, B. (2000). Knowledge management within the context of management: An evolving relationship. *Singapore Management Review,* 22(2), 17.

Martin, A., Dmitriev, D., & Akeroyd, J. (2010). A resurgence of interest in information architecture. *International Journal of Information Management,* 30(1), 6-12.

Mason, D., & Pauleen, D. J. (2003). Perceptions of knowledge management: A qualitative analysis. *Journal of Knowledge Management,* 7(4), 38-48.

Matthew K.O. Lee, Christy M.K. Cheung, Lim, K. H., & Choon, L. S. (2006). Understanding customer knowledge sharing in web-based discussion boards: An exploratory study. *Internet Research,* 16(3), 289-303.

McDermott, R., & O'Dell, C. (2001). Overcoming cultural barriers to sharing knowledge. *Journal of Knowledge Management,* 5(1), 76-85.

Michael, E. (2001). Knowledge management strategies: Toward a taxonomy. *Journal of Management Information Systems,* 18(1), 215-233.

Miesing, P., Kriger, M. P., & Slough, N. (2007). Towards a model of effective knowledge transfer within transnationals: The case of Chinese foreign invested enterprises. *The Journal of Technology Transfer,* 32(1-2), 109-122.

Mir, M. S., Wani, S., & Ibrahim, J. (2013). Critical information security challenges: An appraisal. *2013 5th International Conference on Information and Communication Technology for the Muslim World,* Rabat.

Mittal, S., & Rajib, L. D. (2015). Transformational leadership and employee creativity: Mediating role of creative self-efficacy and moderating role of knowledge sharing. *Management Decision,* 53(5), 894-910.

Mohammad Hossein, I. K., & Nadalipour, Z. (2016). Tourism SMEs and organizational learning in a competitive environment: A longitudinal research on organizational learning in travel and tourism agencies located in the city of Ahvaz, Iran. *The Learning Organization,* 23(2), 184-200.

Mohammadi, K., Khanlari, A., & Sohrabi, B. (2010). Organizational readiness assessment for knowledge management. *Information Resources Management: Concepts, Methodologies, Tools and Applications* (pp. 279-295). New York: Information Science Preference.

Mohr, J. J., & Sengupta, S. (2002). Managing the paradox of inter-firm learning: The role of governance mechanisms. *Journal of Business & Industrial Marketing,* 17(4), 282-301.

Mueller, J. (2014). A specific knowledge culture: Cultural antecedents for knowledge sharing between project teams. *European Management Journal,* 32(2), 190-202.

Muethel, M., & Hoegl, M. (2016). Expertise coordination over distance: Shared leadership in dispersed new product development teams. In: Peus, C., Braun, S., & Schyns, B., (Eds.), *Monographs in Leadership Lessons from Compelling Contexts* (pp. 327 - 348). Bingley: Emerald Group Publishing Ltd.

Mukherji, P. N. (2000). *Methodology in social research: Dilemmas and perspectives: Essays in honor of ramkrishna mukherjee* (Eds ed.). New Delhi: Sage Publications, Incorporated.

Musulin, J., Gamulin, J., & Crnojevac, I. H. (2011). Knowledge management in tourism: The importance of tacit knowledge and the problem of its elicitation and sharing. *Proceedings of the 34th International Convention, MIPRO,* Opatija, 981-987, IEEE.

Myers, M. D. (2013). *Qualitative research in business and management.* London: Sage.

Nakano, D., Muniz, J., & Batista Jr, E. D. (2013). Engaging environments: Tacit knowledge sharing on the shop floor. *Journal of Knowledge Management,* 17(2), 9-9.

Nandi, A. K., Medal, H. R., & Vadlamani, S. (2016). Interdicting attack graphs to protect organizations from cyber attacks: A bi-level defender-attacker model. *Computers and Operations Research,* 75, 118-131.

Nelson, R. R., & Winter, S. G. (2009). *An evolutionary theory of economic change*. London, Harvard University Press.

Neuman, L. W. (2011). *Social research methods: Qualitative and quantitative approaches* (7th ed.). Boston, MA: Pearson Education, Inc.

Newark Beacon Innovation Centre. (2016). Online retailing: Britain, Europe, US and Canada. Retrieved from http://www.retailresearch.org/onlineretailing.php

Newman, G., & McNally, M. M. (2005). *Identity theft literature review*. Washington, DC: National Institute of Justice.

Ni, G., Wang, W., Wang, J., Zong, Z., & Xie, M. (2010). Research on the knowledge management system of the vicarious management corporation. *International Conference of Information Science and Management Engineering,* Xi'an.

Nonaka, I., & Peltokorpi, V. (2006). Objectivity and subjectivity in knowledge management: A review of 20 top articles. *Knowledge and Process Management,* 13(2), 73-82.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science, 5*(1), 14-37.

Nonaka, I., Toyama, R., & Konno, N. (2000). SECI, BA and leadership: A unified model of dynamic knowledge creation. *Long Range Planning,* 33(1), 5-34.

Noor, N. H. M., Ah, Siti Hajar Abu Bakar, & Idris, M. A. (2016). Fostering knowledge sharing through care culture: A comparison study of membership-oriented and service-oriented NGOs in Malaysia. *International Journal of Social Science and Humanity,* 6(7), 489-495.

Noor, N. M., & Salim, J. (2012). The influence of individual, organizational and technological factors on knowledge sharing in the private sector in Malaysia. I*nternational Conference on Information Retrieval & Knowledge Management,* Kuala Lumpur.

Norman K. Denzin, & Yvonna S. Lincoln. (2005). *The Sage Handbook of Qualitative Research.* London: Sage.

O'Keeffe, J., Buytaert, W., Mijic, A., Brozović, N., & Sinha, R. (2016). The use of semi-structured interviews for the characterisation of farmer irrigation practices. *Hydrology and Earth System Sciences,* 20(5), 1911-1924.

Olomolaiye, A., & Egbu, C. (2004). The significance of human resource issues in knowledge management within the construction Industry–People, problems and possibilities. *Proceedings of the Twentieth Annual Conference, Association of Researchers in Construction Management,* Heriot Watt University, 533-540.

Ortega, J. (2001). Job rotation as a learning mechanism. *Management Science,* 47(10), 1361-1370.

Pan, S. L., & Scarbrough, H. (1999). Knowledge management in practice: An exploratory case study. *Technology Analysis & Strategic Management,* 11(3), 359-374.

Pan, S. L., & Scarbrough, H. (1998). A Socio-Technical view of knowledge sharing at buckman laboratories. *Journal of Knowledge Management,* 2(1), 55-66.

Patil, S. J., & Dange, A. (2016). Credit card fraud detection using hidden Markov model. *International Journal of Engineering Science,* 6(4), 3715-3718.

Pawson, R., & Tilley, N. (1997). *Realistic evaluation*. London: Sage.

Pedro Soto-Acosta, & Juan-Gabriel Cegarra-Navarro. (2016). New ICTs for knowledge management in organizations. *Journal of Knowledge Management,* 20(3) 417-422.

Pervaiz, U., Imran, M., Arshad, Q., Haq, R., & Khan, M. K. (2016). Human resource practices and knowledge sharing: The moderating role of trust. *International Journal of Organizational Leadership,* 5(1), 15-23.

Peter A.C. Smith. (2012). The importance of organizational learning for organizational sustainability. *The Learning Organization,* 19(1), 4-10.

Pilat, L., & Kaindl, H. (2011). A knowledge management perspective of requirements engineering. *Fifth International Conference on Research Challenges in Information Science,* Gosier, 1-12.

Poynder, R. (1998). Getting to the nuts and bolts of knowledge management. *Information World Review,* 135(135), 20.

Preston, J., Swan, J., & Scarbrough, H. (1999). *Knowledge management: a literature review.* London, Institute of Personnel and Development.

Pyrooz, D. C., Decker, S. H., & Moule, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the internet. *Justice Quarterly,* 32(3), 471-499.

Reeves, C. L. (2010). A difficult negotiation: Fieldwork relations with gatekeepers. *Qualitative Research,* 10(3), 315-331.

Reid, F. (2003). Creating a knowledge-sharing culture among diverse business units. *Employment Relations Today,* 30(3), 43.

Reyns, B. W. (2013). Online routines and identity theft victimization further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency,* 50(2), 216-238.

Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology,* 1-21.

Rezaei, S., & Wan Ismail, W. K. (2014). Examining online channel selection behaviour among social media shoppers: A PLS analysis. *International Journal of Electronic Marketing and Retailing,* 6(1), 28-51.

Rice, J. L., & Rice, B. S. (2005). The applicability of the SECI model to multi-organisational endeavours: An integrative review. *International Journal of Organisational Behaviour,* 9(8), 671-682.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems,* 11(3), 271-295.

Riege, A. (2005). Three-dozen knowledge-sharing barriers managers must consider. *Journal of Knowledge Management,* 9(3), 18-35.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation,* 35, 22-31.

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (2013). *Qualitative research practice: A guide for social science students and researchers.* Sage.

Robertson, M., & O'Malley Hammersley, G. (2000). Knowledge management practices within a knowledge-intensive firm: The significance of the people management dimension. *Journal of European Industrial Training,* 24(2/3/4), 241-253.

Robinson, J. (2011). Transparency and confidence-building measures for space security. *Space Policy,* 27(1), 27-37.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management,* 30(2), 256-286.

Roth, J., & Broad, E. (2008). The speed of trust: The one thing that changes everything. *People & Strategy,* 31(1), 57-58.

Rubin, A., & Babbie, E. R. (2016). *Empowerment series: Research methods for social work*. Boston: Cengage Learning.

Rulke, D. L., & Galaskiewicz, J. (2000). Distribution of knowledge, group network structure, and group performance. *Management Science,* 46(5), 612-625.

Rutten, W., Rutten, W., Blaas-Franken, J., Blaas-Franken, J., Martin, H., & Martin, H. (2016). The impact of (low) trust on knowledge sharing. *Journal of Knowledge Management,* 20(2), 199-214.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security,* 2016(2), 15-18.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior,* 57, 442-451.

Saha, P., Bose, I., & Mahanti, A. (2016). A knowledge based scheme for risk assessment in loan processing by banks. *Decision Support Systems,* 84, 78-88.

Sakharova, I. (2012). Payment card fraud: Challenges and solutions. *International Conference on Intelligence and Security Informatics,* Arlington.

Salleh, K. (2010). Tacit knowledge and accountants: Knowledge sharing model. *Second International Conference on Computer Engineering and Applications,* Bali Island.

Santos, R. E., da Silva, F. Q., de Magalhães, C. V., & Monteiro, C. V. (2016). Building a theory of job rotation in software engineering from an instrumental case study. *Proceedings of the 38th International Conference on Software Engineering,* Austin, 971-981, SCM.

Sarmento, A. (2005). Knowledge management: At a cross-way of perspectives and approaches. *Information Resources Management Journal,* 18(1), 1-7.

Schlegelmilch, B. B., & Chini, T. C. (2003). Knowledge transfer between marketing functions in multinational companies: A conceptual model. *International Business Review,* 12(2), 215-232.

Scott Holste, J., & Fields, D. (2010). Trust and tacit knowledge sharing and use. *Journal of Knowledge Management,* 14(1), 128-140.

Searle, J. R. (1985). *Expression and meaning: Studies in the theory of speech acts.* Cambridge: Cambridge University Press.

Shah, M., & Okeke, R. I. (2011). A framework for internal identity theft prevention in retail industry. *2011 European Intelligence and Security Informatics Conference,* Athens.

Shaobo Ji, Jianquan Wang, Qingfei Min, & Smith-Chao, S. (2007). Systems plan for combating identity theft - A theoretical framework. *International Conference on Wireless Communications, Networking and Mobile Computing,* Shanghai.

Shapero, A. (1985). *Managing professional people: Understanding creative performance*. London: Collier Macmillan.

Shaw, R., Opalkar, U., Mathur, N., & Manjula, R. (2016). Analysis of web phishing methods. *International Journal of Science and Research,* 5(5), 566-576

Sheehan, M. (2016). Leadership style and behaviour, employee knowledge-sharing and innovation probability. In Shipton, H., et al*.,* (Eds.), *Human resource management, innovation and performance* (pp. 179-196), Hampshire: Palgrave Macmillan, UK.

Silverman, D. (2013). *Doing qualitative research* (4th ed.). London: Sage.

Silvi, R., & Cuganesan, S. (2006). Investigating the management of knowledge for competitive advantage: A strategic cost management perspective. *Journal of Intellectual Capital,* 7(3), 309-323.

Singh Sandhu, M., Kishore Jain, K., & Umi Kalthom bte Ahmad, Ir. (2011). Knowledge sharing among public sector employees: Evidence from Malaysia. *International Journal of Public Sector Management,* 24(3), 206-226.

Siong, C. C., Salleh, K., Syed Noh, S. A., & Syed-Ikhsan Syed, O. S. (2011). KM implementation in a public sector accounting organization: An empirical investigation. *Journal of Knowledge Management,* 15(3), 497-512.

Sloan, S., Bodey, K., & Richard Gyrd-Jones. (2015). Knowledge sharing in online brand communities. *Qualitative Market Research: An International Journal,* 18(3), 320-345. doi:10.1108/QMR-11-2013-0078

Smith, H. W. (1981). *Strategies of social research: The methodological imagination.* New Jersey: Prentice Hall.

Smith, A. D. (2008). Modernizing retail grocery business via knowledge management-based systems. *Journal of Knowledge Management,* 12(3), 114-126.

Song, S. (2002). An internet knowledge sharing system. *The Journal of Computer Information Systems,* 42(3), 25.

Stahle, P. (1999). New challenges for knowledge management. In Reeves, J. (Ed.) *Liberating Knowledge* (pp. 36-42). London: Caspian Publishing.

Stake, R. E. (1995). *The art of case study research*. London: Sage.

Stankosky, M. (2005). *Creating the discipline of knowledge management: The latest in university research*. London: Routledge.

Starovic, D., & Marr, B. (2003). *Understanding corporate value: Managing and reporting intellectual capital cima.* Cranfield University School of Management, UK.

Stenmark, D. (2000). Leveraging tacit organizational knowledge. *Journal of Management Information Systems,* 17(3), 9-24.

Stephen Harrison. (2013). Annual fraud indicator, March 2012. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf

Stoddart, L. (2001). Managing intranets to encourage knowledge sharing: Opportunities and constraints. *Online Information Review,* 25(1), 19-29.

Storey, J., & Barnett, E. (2000). Knowledge management initiatives: Learning from failure. *Journal of Knowledge Management,* 4(2), 145-156.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research.* Newbury Park, CA: Sage.

Suppiah, V., & Singh Sandhu, M. (2011). Organisational culture's influence on tacit knowledge-sharing behaviour. *Journal of Knowledge Management,* 15(3), 462-477.

Sveiby, K. (2001). A knowledge-based theory of the firm to guide in strategy formulation. *Journal of Intellectual Capital,* 2(4), 344-358.

Syed Omar, S. S., & Rowland, F. (2004). Knowledge management in a public organization: A study on the relationship between organizational elements and the

performance of knowledge transfer. *Journal of Knowledge Management,* 8(2), 95-111.

Syed-Ikhsan, S. O. S., & Rowland, F. (2004). Knowledge management in a public organization: A study on the relationship between organizational elements and the performance of knowledge transfer. *Journal of Knowledge Management,* 8(2), 95-111.

Szulanski, G. (2000). The process of knowledge transfer: A diachronic analysis of stickiness. *Organizational Behavior and Human Decision Processes,* 82(1), 9-27.

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. *New England Journal of Medicine,* 368(11), 977-979.

Tangaraja, G., Mohd Rasdi, R., Abu Samah, B., Ismail, M., Chase, R., & Chase, R. (2016). Knowledge sharing is knowledge transfer: A misconception in the literature. *Journal of Knowledge Management,* 20(4)

Taylor, D. W., Yamamura, J., Stedham, Y., & Nelson, M. (2001). Managing knowledge workers in accounting firms: The role of nutrient information and organizational information consciousness. *Journal of Knowledge Management Practice,* 2(July), 1-15.

Thabatah, F., Dahal, K., Hossain, M., & Aburrous, M. (2010). Experimental case studies for investigating E-banking phishing intelligent techniques and attack strategies. *Journal of Cognitive Computation,* 2(3), 242-253.

Thoben, K., Weber, F., & Wunram, M. (2001). Towards pragmatic approaches for knowledge management in Engineering–Theory and industrial applications. *Proceedings of 13th International Conference on Engineering Design,* Glasgow.

Titi Amayah, A. (2013). Determinants of knowledge sharing in a public sector organization. *Journal of Knowledge Management,* 17(3), 454-471.

Tohidinia, Z., & Mosakhani, M. (2010). Knowledge sharing behaviour and its predictors. *Industrial Management & Data Systems,* 110(4), 611-631.

Tony, N. (2013). How to prevent identity theft. Retrieved from http://www.bbc.co.uk/consumer/22342924

Triggs, D. D., & King, P. M. (2000). Job rotation. *Professional Safety,* 45(2), 32.

Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory framework. *The Journal of Strategic Information Systems,* 21(1), 1-17.

Ur-Rahman, N., & Harding, J. A. (2012). Textual data mining for industrial knowledge management and text classification: A business oriented approach. *Expert Systems with Applications,* 39(5), 4729-4739.

Usoro, A., Sharratt, M. W., Tsui, E., & Shekhar, S. (2007). Trust as an antecedent to knowledge sharing in virtual communities of practice. *Knowledge Management Research & Practice,* 5(3), 199-212.

Valentine St Leon, M. (2002). Intellectual capital: Managerial perceptions of organisational knowledge resources. *Journal of Intellectual Capital,* 3(2), 149-166.

Van den Hooff, B., Elving, W., Meeuwsen, J. M., & Dumoulin, C. (2003). Knowledge sharing in knowledge communities. In: M. Huisman et al*.,* (Eds.), *Communities and Technologies* (pp. 119-141). Netherlands: Springer.

Van Knippenberg, D., De Dreu, C. K., & Homan, A. C. (2004). Work group diversity and group performance: An integrative model and research agenda. *Journal of Applied Psychology,* 89(6), 1008.

Vieraitis, L. M., Copes, H., Powell, Z. A., & Pike, A. (2015). A little information goes a long way: Expertise and identity theft. *Aggression and Violent Behavior,* 20, 10-18.

Vlăduțescu, Ș. (2014). Uncertainty communication status. *International Letters of Social and Humanistic Sciences,* (21), 100-106.

Wang, W., & Hou, Y. (2015). Motivations of employees' knowledge sharing behaviors: A self-determination perspective. *Information and Organization,* 25(1), 1-26.

Wang, S., & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. *Human Resource Management Review,* 20(2), 115-131.

Wei'e, W. (2011). Analysis of knowledge transfer process and model building. *International Conference on E-Business and E-Government,* Shanghai, 1-4.

Wenger, E. (1998). Communities of practice: Learning, meaning, and identity. Cambridge: Cambridge University Press.

Wenger, E., McDermott, R. A., & Snyder, W. (2002). *Cultivating communities of practice: A guide to managing knowledge*. Boston: Harvard Business School Press.

Wengraf, T. (2001). *Qualitative research interviewing: biographic narrative and semi-structured interviewing.* London: Sage.

WenJie Wang, Yufei Yuan, & Archer, N. (2006). A contextual framework for combating identity theft. *Security & Privacy,* 4(2), 30-38.

White, R. S. (2001). Working knowledge: How organizations manage what they know. *The Journal of Technology Transfer,* 26(4), 396-397.

White, M. D., & Fisher, C. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review,* 19(1), 3-24.

Willem, A., & Buelens, M. (2007). Knowledge sharing in public sector organizations: The effect of organizational characteristics on interdepartmental knowledge sharing. *Journal of Public Administration Research and Theory,* 17(4), 581-606.

Willem, A., & Buelens, M. (2009). Knowledge sharing in inter-unit cooperative episodes: The impact of organizational structure dimensions. *International Journal of Information Management,* 29(2), 151-160.

Wilson, J. (2014). *Essentials of business research: A guide to doing your research project* (2nd ed.). London: Sage.

Wong, Y., Maher, T. E., Nicholson, J. D., & Bai, A. F. (2003). Organisational learning and the risks of technology transfers in china. *Management Research News,* 26(12), 1-11.

Xu, E., Zheng, P., Wu, X., & Zhang, X. (2006). The effects of organizational factors on knowledge sharing. *International Conference on Management Science and Engineering,* Lille, 1256-1261.

Yahya, S., & Wee-Keat Goh. (2002). Managing human resources toward achieving knowledge management. *Journal of Knowledge Management,* 6(5), 457-468.

Yan Li, & Zetian Fu. (2007). A framework of knowledge transfer process in expert system development. *International Conference on Wireless Communications, Networking and Mobile Computing,* Shanghai, 5597-5600. doi:10.1109/WICOM.2007.1371

Yang, S., & Farn, C. (2009). Social capital, behavioural control, and tacit knowledge sharing-A multi-informant design. *International Journal of Information Management,* 29(3), 210-218.

Yang, J. (2007). Knowledge sharing: Investigating appropriate leadership roles and collaborative culture. *Tourism Management,* 28(2), 530-543.

Yao, L., Kam, T., & Chan, S. H. (2007). Knowledge sharing in Asian public administration sector: The case of Hong Kong. *Journal of Enterprise Information Management,* 20(1), 51-69.

Yen-Ku Kuo, Tsung-Hsien Kuo, & Li-An Ho. (2014). Enabling innovative ability: Knowledge sharing as a mediator. *Industrial Management & Data Systems,* 114(5), 696-710.

Yildirim, E. (2016). The importance of information security awareness for the success of business enterprises. *Advances in Human Factors in Cybersecurity* (pp 211-222). Springer International Publishing.

Yin, R. K. (2011). *Applications of case study research.* London: Sage.

Yin, R. K. (2014). *Case study research: Design and methods.* London: Sage.

Yin, R. K. (2015). *Qualitative research from start to finish* (2nd ed.). London, Guilford Publications.

Zahedi, M., Shahin, M., & Babar, M. A. (2016). A systematic review of knowledge sharing challenges and practices in global software development. *International Journal of Information Management,* 36(6), 995-1019.

Zakaria, O. (2006). Internalisation of information security culture amongst employees through basic security knowledge. In: Fischer-Hübner, S. et al*.,* (Eds.) Security *and privacy in dynamic environments* (pp. 437-441). Boston: Springer.

Zander, U., & Kogut, B. (1995). Knowledge and the speed of the transfer and imitation of organizational capabilities: An empirical test. *Organization Science,* 6(1), 76-92.

Zhao Sheng-hui. (2010). Information resources security of library knowledge transfer under network environment paper. *International Conference on E-Product E-Service and E-Entertainment,* Henan.

Appendix A: Research Instrument of the Study

Questions Asked	Sample Probe/ Further Questions
Block 01: About Interviewee	
What are your work responsibilities related to information security in the organisation?	Job title
How long have you been working in the organisation in that position?	In what departments and groups?
Block 02: KM Infrastructure	
What are the tools being used for sharing the knowledge for ID theft prevention in the organisation?	What IT skills are you required to have for sharing the knowledge for ID theft prevention?
How satisfied are you with the availability of the existing resources in your organisation for sharing the knowledge for ID theft prevention?	If not, then why?
To what extent are you satisfied with the usage of the existing resources provided in your organisation for the knowledge sharing for ID theft prevention?	If not, then what are the reasons?
What other resources would you like to have available to you?	
Block 03: ICT Know-how and Training	
How do you provide training to workers for enhancing their knowledge sharing skills for ID theft prevention in your organisation? (for managers only)	How do you get training to enhance your skills for knowledge sharing for ID theft prevention in your organisation? (for employees)
What advantages do you get from the training given for knowledge sharing for ID theft prevention in your organisation?	How do you implement the knowledge given in training for knowledge sharing for ID theft prevention?
Are these learning opportunities useful to you for sharing knowledge for ID theft prevention?	If yes, then how?
Block 04: Job Rotation	
Does your organisation practice job rotation to increase the knowledge of the employees?	If no, then why?
How useful is job rotation for increasing the knowledge of the employees for the prevention of ID theft in your organisation?	How do individuals gain an advantage of knowledge sharing for ID theft prevention from job rotation? How do teams get the benefit from job rotation for the knowledge sharing for ID theft prevention?
Block 05: Feedback on Performance Evaluation	
How does your organisation evaluate the performance of employees for the knowledge sharing for ID theft prevention?	If not, then why?
How does feedback on the performance of employees' impact on the knowledge sharing for ID theft prevention in your organisation?	
Block 06: Information Sourcing Opportunities	
Which information sources are provided to you for sharing the knowledge for ID theft prevention? (Email, internal network messaging, policy documents, text messages on cell phones).	Which of these resources do you prefer to use? Why? Which of these sources do you get the most up-to-date information from?
What other sources do you require for the knowledge sharing for ID theft prevention in the organisation?	
Block 07: Leadership Support	
How does management share the knowledge for ID theft prevention with employees in the organisation? (for managers only)	In what way do you receive information for ID theft prevention? (for employees)

What support do you expect from top management of your organisation for the knowledge sharing for ID theft prevention?	
Block 08: Knowledge Sharing Culture	
Do you trust others concerning the knowledge sharing for ID theft prevention in your organisation?	If no, then why?
Do you share knowledge concerning ID theft prevention with your colleagues in the organisation?	Do others, such as your colleagues in the same department or in other departments, share the knowledge for ID theft prevention with you?
What cultural changes (such as trust of other employees, communication with others and the behaviour of the information system) do you consider to be effective for the knowledge sharing for ID theft prevention in the organisation?	