An evaluation of inter-organisational identity theft knowledge sharing practice in the UK retail sector

by

Rozina Chohan

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

November 2016

uclan
University of Central Lancashire

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

---

Signature of Candidate

Type of Award **Doctoral of Philosophy**

School **School of Business**

Acknowledgements

I would like to acknowledge the support and guidance of my director of studies Dr Mahmood Shah, and supervisors Dr Mary Welch and Dr Mitchell Larson for their advice and encouragement. I am grateful for the support and encouragement from Professor Waqar Ahmed.

I am eternally grateful to my parents Mir Muhammad and Morezadi Chohan for their love, encouragement, sacrifice and endless support. Without their unwavering support none of this work would have been possible. To them I dedicate my life and work.

I also appreciate the love and the fun times I have had with my brothers, Imran and Irfan and sisters, Rubina, Farhana, Murk and Sehrish. I especially love my nephews, Ayan and Zain; you have made my life a joy.

I would like to acknowledge the support and encouragement of my research room colleagues, Doreen, Rateb, Hamis, Pakistani research group, Indonesian and Libyan friends and all other nationalities.

My appreciation also goes to the companies who have devoted their time and efforts unselfishly to provide me with information and data that have made this work possible.

Government of Pakistan and Shah Abdul Latif University, Khairpur thanks for choosing me to study abroad.

Abstract

Knowledge is an essential source of competitive advantage in modern society and is particularly important in the current on-line environment due to increased business interactions throughout the world. Knowledge sharing initiatives taken by organisations to improve technicalities to tackle cyber threat have been extensively investigated. A particular focus of this study was on the security professionals sharing their learning experience in order to help address and mitigate identity theft. Multiple case studies were employed to interpret the triangulated data collected. ShoppingCo, PaymentCo, TeleCo, and NetworkingCo participated in this investigation. Semi structured interviews were scheduled and conducted in conjunction to company reports, personal communication, presentation slides and related materials was gathered to ensure trustworthiness and authenticity. Pattern matching analysis was employed to draw conclusions by evaluating 30 transcripts and 11 internal documents.

The major theoretical contribution of this study was the proposal of a conceptual framework that adapts for private sector organisations knowledge sharing elements in the security profession. Lack of knowledge of the manager’s role is addressed. Current knowledge sharing and corporate communication practices are synthesised. Formal and informal communication, social forums and networking events are evaluated. Thus, improving the current understanding of identity theft.

This empirical study contributes to an improved understanding of inter-organisational knowledge sharing practice within three retailers and an official networking forum. Because of this evaluation, an extended framework is proposed and components synthesised into a new framework. Recommendations are drawn based on an evaluation of what is working and what does not seem to be providing benefits with regard to knowledge that address and mitigate identity theft. The framework suggested that the key to improved knowledge sharing was to persuade a range of security officials working for different private sector organisations to share their knowledge of identity theft prevention.

Table of content

List of Figures

List of Tables

Abbreviations

CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSSC	Cross-sector Safety and Security Communications
CVV	Card Verification Value
DNA	deoxyribonucleic acid
FACTA	Fair and Accurate Transaction Act
FCA	Financial Conduit Authority
GLBC	Gramm-Leach Bliley Act
KM	Knowledge Management
KS	Knowledge Sharing
ISF	Information Security Forum
IP	Internet Protocol
IS	Information Security
IC	Inter-organisational communication
ICT	Information Communication Technology
ISO	International Organisations for Standardisation
ISVC	Information Security Virtual Community
IT-ISAC	Information Technology – Information Sharing and Analysis Centre
IT	Information Technology
MD	Managed Delivery
MOPAC	Mayor of London Office for Policing and Crime
NCA	National Crime Agency
NFIB	National Fraud Intelligence Bureau
OBJ	Research Objective
PCI	Payment Card Industry Data Security Standard (PCI DSS)
PIN	Personal Identification Number
QNo.	Interview Guide Question Number
S.No.	Serial Number
RIPA	Regulation of Investigatory Power Act
RQ	Key Research Question
RPA	Research Program Approval
RSS	Rich Site Summary

SECI	Socialisation, Externalisation, Commination and Internalisation
SME	Small Medium Enterprises
SSL	Secure Socket Layer
TSCM	Technical Surveillance Counter Measure
UK	The United Kingdom
URL	Uniform Resource Locator
USA	The United States of America

CHAPTER 1 INTRODUCTION

This chapter describes the research background, aim and objectives of the study and key research questions. The rationale behind work is discussed followed by the contribution of the project to knowledge sharing practice and concludes with thesis structure.

1.1 Research Background

Identity theft is a global problem (Roberts, 2012). The United Kingdom (UK), like many of the developed countries spends considerable amount of money and human resource on trying to enhance cyber security, and find ways to prevent crimes related to identity theft (Khan, 2015). For instance, Cross-sector Safety and Security Communication (CSSC) is a charitable hub in the UK that aims to help businesses remain safe and secure, regardless whether an organisation belongs to the public or private sector. CSSC covers over thirty sectors in the UK including accountancy, hotel, media, post office, travel, banking, information technology, telecommunications, London Boroughs and Resilience, tourism, insurance, law, food and supply chain, pharmaceutical, transport, security, construction, retail and wholesale (See http://www.vocal.co.uk/cssc/wp-content/uploads/2012/04/Industry-Diagram.png). Cifas no abbreviation (Previously CIFAS – stands for Credit Industry Fraud Avoidance System) is a leader in fraud prevention in the UK to support a number of organisations in these sectors by providing intelligence-sharing systems. In spite of these collective efforts, however, the extent of identity frauds is continuing to increase. A recent report produced by Cifas to measure fraud incidences recorded in 2014 (Cifas, 2015a) indicates a 25% increase in frauds from 2013. Trustwave's 2013 Global Security Report shows retailing as the most compromised industry with 45% of the incidents (Trustwave, 2013, p. 9). The report also indicated that the UK is the fourth most victimised country after United States, Australia, and Canada (p. 7). Online frauds against UK retailers is estimated £105.5 million in the year 2013 which is increased by 4% from previous year (Khan, 2015, p. 16).

Retailing is "*the business of selling goods and/or services directly to consumers*" (Church, 2014, p. 89). However, it is difficult to use single definition of retailing because it involves a vast array of entities (Laudon and Traver, 2013; Rabolt and Miler, 2009). For instance, there are business-to-consumer (B2C), business-to-business (B2B), consumer-to-consumer (C2C), and social, mobile and local retailing outlets (Laudon and Traver, 2013). These outlets use various channels such as departmental stores, grocery, mail order and online retail (Marciniak and Bruce, 2004). This study concentrates on the online retail, because it is the most prone channel to identity theft. Nearly, 82% of frauds are committed online (Cifas, 2015c).

Over the past decade, most retailers in the UK were reluctant to use Internet technologies to run business and have been using the traditional style of "bricks and mortar" outlet (Marciniak and Bruce, 2004, p. 368). However, this conventional method still exists; online retailing is growing rapidly as an easier means of supporting business activities (MarketLine, 2015). For instance, businesses are now merging and eliminating non-profitable units to utilise Information Technology (IT) as the key driver incorporating services of delivery companies to bring shopping to the doorsteps of customers (Rabolt and Miler, 2009). Doherty and Hart (1999) predicted that the use of technology such as the Internet might replace the high street stores. eBay and Amazon are bringing their prediction to fruition. Conventional retailers, such as, Debenhams, Next Plc, Sainsbury's Grocery and Tesco, are also using online mechanisms to supplement their traditional ways of trading.

Shifting of the businesses activities from onsite to online not only reduces retailers' cost, but also improves staff productivity, and is more convenient for the customers (Aerohive Networks, 2013; Liefeld, 2013). Online retailers expand their reach (Choo, 2011), and attract consumers' attention to the new pricing offers because of the reduced cost (MarketLine, 2015; Doherty, Ellis-Chadwick and Hart, 1999). Therefore, online retailers are contributing significantly to the UK's economy, are being more widely appreciated by the society (Rudrabasavaj, 2010).

However, the use of these technologies as a vehicle in business not only assists business and consumers' interaction but also malicious actors' (Xu, 2012; Geeta, 2011). Abuse of identity information is a common problem which increases with the use of advanced technology and devices such as laptops, smart phones and tablets (Bose and Leung, 2013).

For instance, Internet technologies can completely transform business with the use of digital transactions and information control systems (Laudon and Traver, 2013, 51; Domaleski, 2000, p. 2). This information system is composed of personally identifiable information of business employees, customers and partners (Geeta, 2011). Virtual communication between businesses and consumers enables potential criminals to steal consumers' and even business information as noted in the theory of criminology (Prabowo, 2011). Crime occurs when motivated offenders are able to access targets in the absence of guardians who can intervene (Cohen and Felson, 1979). These elements are associated with online retailing which is incapable of "seeing" likely offenders due to the virtual interaction with customers. This communication provides fraudsters with the opportunity to attack business information systems by hacking, phishing and scamming to steal customers' details (Geeta, 2011; Prabowo, 2011). Criminals either use the same information or modify slightly to perpetuate their online criminal activities (Cifas, 2014b; Cifas, 2015b).

In response to cybercriminals, a holistic information security management approach has advised to take into account human elements (Flores, Antonsen and Ekstedt, 2014). Therefore, prevention, detection, analysis and prosecution are commonly considered in organisations to ensure information security (Ahmad, Maynard and Park, 2014; Wilhelm, 2004). Identity theft or frauds have risen because of extensive use of technology. Literature therefore pays less attention to knowledge sharing as a strategic practice to enhance security officials' technical abilities (Easterby-Smith and Prieto, 2008; Easterby-Smith and Lyles, 2011; Tsoukas, 2011). Identity theft prevention knowledge is not widely shared amongst security professional (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013). Intelligence sharing reports indicate that fraud knowledge is being communicated among the companies (Cifas, 2014b; Cifas, 2015b). However, little literature is available in academic journals that focus information security knowledge sharing practice very broadly (Flores, Antonsen and Ekstedt, 2014; Feledi, Fenz and Lechner, 2013; Liu, Ji and Mookerjee, 2011). The limited research in knowledge sharing may be attributed to technicalities associated with identity theft prevention.

Therefore, to extend knowledge in information security knowledge sharing literature, this study focused on establishing how security professionals can enhance fraud prevention knowledge through sharing learning experiences. Security officials need to be ‘proactive’ to reduce ‘wheel-reinvention’ in order to decrease the adverse impact of identity theft (Lopez and Esteves, 2013, p. 99). A knowledge sharing practice may be helpful to companies to produce better solutions in a timely and cost-effective manner (Nonaka *et al.*, 2014). These challenges posed in the current literature regarding these issues are examined in this thesis.

1.2 Aims and Objectives

Aims

The aims of this study is:

To evaluate inter-organisational knowledge sharing surrounding identity theft prevention and to propose a holistic knowledge-sharing framework in this profession.

The aims further broken down into the following objectives to investigate the study adequately.

Objectives

- *To investigate various identity fraud prevention practices by reviewing the literature and published reports. (OBJ1)*

- *To investigate existing knowledge sharing within companies across a broad spectrum of business presented in the open literature. (OBJ2)*

- *To select a suitable business to investigate based on the knowledge and understanding obtained from rigorous literature review and analysis. (OBJ3)*

- *To assess how different organisations share identity fraud prevention knowledge with each other by investigating knowledge sharing practices within three organisations in the retail industry and with a networking forum. (OBJ4)*

- *To propose an extended knowledge sharing framework within the security profession. (OBJ5)*

1.3 Research Questions

Limited literature in information security knowledge sharing practice (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Liu, Ji and Mookerjee, 2011; Tamjidyamcholo *et al.*, 2014), and intelligence sharing reports (Trustwave, 2013; Cifas, 2015b; Cifas, 2016) suggest that the businesses have ample opportunities to share fraud prevention knowledge. Cifas members are provided with a number of offline opportunities to collaborate several times a year nationally and locally (Cifas, 2014a) and National Fraud Database (NFD) is shared centrally. Various online forums exist focusing on information security profession such as Information Security Forum (ISF) and Information Technology – Information Sharing and Analysis Centre (IT-ISAC) where security officials collaborate with one another. Despite these collective efforts, however, several questions remain unanswered including: Why is there growing concern in the increase on identity frauds (Trustwave, 2013; Cifas, 2015b)? What obstructs security professionals from improving their technicalities through sharing learning experiences to address and mitigate identity theft? These challenges, prompted several research questions including the following:

1. *What is working in the retail sector and what does not seem to be providing benefit with regard to knowledge sharing to address and mitigate identity theft? (RQ1)*

2. *To what extent are companies willing to share fraud prevention knowledge with each other and under which condition(s)? (RQ2)*

3. *Why do some individual either not take part or have little active participation in information security knowledge sharing? (RQ3)*

RQ1 and RQ2 are designed based on gaps in the literature discussed (Section 2.5) and RQ3 is adopted from Tamjidyamcholo *et al*. (2014, p. 31) who discovered that some professional either do not participate or have less interest to contribute their knowledge in the online professional communities such as LinkedIn. RQ1 concentrates on effectiveness and efficiency of communication tools and techniques that security officials use to share security-related knowledge. These questions contain two components broken down as follows:

> RQ1 (a): What is working for retailers with regards to knowledge sharing to address and mitigate identity theft?
>
> RQ1 (b): What does not seem to be providing benefit with regards to knowledge sharing to address and mitigate identity theft?

RQ2 and RQ3 focus on security officials' behavioural and relational factors and their reaction to the knowledge sharing processes based on trust and associated risk. Similar to RQ1, RQ2 has two components as follows:

> RQ2 (a): To what extent are companies willing to share fraud prevention knowledge with each other?
>
> RQ2 (b): Under which condition(s) are companies willing to share fraud prevention knowledge with each other?

RQ3 can be broken down into two parts as:

> RQ3 (a) Why do some security officials not take part in information security knowledge sharing?
>
> RQ3 (b) Why do some security officials have small active participation in information security knowledge sharing?

The literature review conducted as part of this thesis suggests several shortcomings in the domain of information security knowledge sharing surrounding identity fraud. For instance, Tamjidyamcholo *et al*. (2013, p. 223) pointed out that: "*Despite the importance of information security, little research based on knowledge sharing has focused on the security profession*". Therefore, these authors investigated an Information Security Virtual Community (ISVC) to explore intentions and attitudes associated with members of the community with respect to trust, self-efficacy, and reciprocity and shared language. However, these predictors are not all inclusive for generalising information security professionals' knowledge sharing activities. More work is required to consider social interactions, personal outcome expectations, altruism and shared vision (Tamjidyamcholo *et al.,* 2013, p. 231). Knowledge sharing between organisations is not a simple phenomenon (Yang and Maxwell, 2011; Bigdeli, Kamal and Cesare, 2013) as this involves multifaceted nature of boundaries, processes, cultures, confidentiality, leakage, communication skills, tools, institutionalised routines and social capital (Styhre, 2011; Szulanski, 1996; Easterby-Smith, Lyles and Tsang, 2008). This phenomenon requires an understanding of inter-organisational knowledge sharing practice and the associated components affecting the knowledge sharing process. This understanding can improve knowledge sharing capabilities of online businesses (Easterby-Smith, Lyles and Tsang, 2008). Therefore, a framework of all-inclusive components may assist in this understanding (Tamjidyamcholo *et al.*, 2013). Motivated by these challenges the following research question was designed:

> **4.** *Which is the suitable knowledge sharing framework in the security profession in retail that facilitates an understanding of inter-organisational identity theft prevention knowledge sharing practice? (RQ4)*

RQ4 covers a framework of all-inclusive components that affect information security knowledge sharing. This study chose a framework of factors influencing inter-organisational knowledge transfer to evaluate how retail sector address and mitigate identity theft via sharing learning experiences from peers (Easterby-Smith, Lyles and Tsang, 2008). Details of this framework such as its selection, suitability, applicability, reliability and comparison with other frameworks are explained in Chapter 3. This thesis proposes that corporate communication requires a knowledge that is flowing fluidly and an interactive environment to facilitate security professionals to learn from each other's experiences.

1.4 Research Methodology

Most studies in the security profession evaluated knowledge sharing practice through surveys (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Tamjidyamcholo *et al.*, 2014). A general limitation of this method is that constructs associated with behavioural information security governance to establish security knowledge sharing initiatives may not be effectively measured with the use of surveys (Flores, Antonsen and Ekstedt, 2014, p. 106). For instance, Pérez-Nordtvedt *et al.* (2008, p. 738) discovered that *"A survey-based approach to measurement cannot fully capture the richness and social complexity of knowledge transfer process*". An investigation of inter-organisational knowledge sharing process requires qualitative case studies (Easterby-Smith, Lyles and Tsang, 2008). Carefully designed multiple case studies appear to be a logical step in advancing this line of inquiry (Pérez-Nordtvedt *et al.*, 2008). To overcome methodological limitations, this study employs qualitative case studies incorporating literature review analysis and semi-structured interviews.

Yin's (2009) case study methodology is employed to collect and analyse the data. Inter-organisational knowledge sharing practice by definition involves minimum of two organisations (Easterby-Smith, Lyles and Tsang, 2008, p. 679); therefore, a multiple case study design approach is designed to understand knowledge sharing between the online retailers. Purposive sampling criterion was used to explore relevant insights. In doing so, security officials in the retail sector were contacted due to their front line experiential knowledge of identity theft related problems (Flores, Antonsen and Ekstedt, 2014). They have provided appropriate information to dictate their learning experiences to address and mitigate identity theft. The online businesses were chosen in retail due to the fact that online is the most widely used channel for committing identity fraud (Cifas, 2015c). Therefore, security officials in these organisations found more knowledgeable in addressing the research questions posed. Cifas (2015b) fraudscape supports this assumption that online retailers are more prone to identity theft.

From the title of this study, it is clear that it requires face-to-face interactions with security professionals to gain insights in the real setting. Therefore, one-to-one interviews with knowledge holders were conducted. Semi-structured interviews, informal meetings, field notes, non-participant observation, industry's internal briefings and documented data were collected during the field visits. Thematic coding technique was used to organise large volume of the data. Themes presented were based on the components of the framework synthesised in Chapter 2 and 3. The analysis is reported based on research questions (Chapter 5). Employing pattern matching extends the framework (Chapter 6).

1.5 Focus of the Study

This study chose to investigate identity theft and fraud associated with consumers' identity details. Business information systems consist of various invaluable assets such as intellectual property, competitive assets (specialised knowledge), client confidential information, and internal private information such as payroll and salary (Ahmad, Maynard and Park, 2014, p. 366). Since there is limited literature available to prevent identity theft (Okeke, 2015), this is a useful research domain for further investigation. The studies conducted to evaluate how to secure business information system may explicitly contribute to secure identity information. However, very few studies focused online businesses (Roberts, 2012; Finch, 2011; Finch, 2007). Therefore this thesis considers knowledge sharing practice between in online retail as a novel contribution (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Tamjidyamcholo *et al.*, 2014).

1.6 Significance of the Study

This study contributes to the literature in following ways. Firstly, this is an original work based on real cases. Insights are gained from real actor working in the security profession. Secondly, it links a number of research areas together such as information security, knowledge management and corporate communication. It provides new insights on how these three broader areas can complement one another to mitigate identity theft. However, its contribution is not limited to identity theft prevention. Knowledge sharing practices identified in this thesis and the anecdotes from the respondents are valuable contributions to the literature in online information security. Knowledge management practitioners and communication theorists may find it useful.

The main contribution of this thesis is a holistic model of underlying practices that prevent identity theft (Figure 5-1). In particular, a framework of the factors influencing inter-organisational knowledge sharing practice (Figure 3-3) is applied, evaluated and extended as new model in the security profession (Figure 6-1). Such an extension is a novel contribution to existing body of knowledge and improves managerial and organisational practices with regards to sharing fraud prevention knowledge to advance professionals' abilities in the online retail.

1.7 Thesis Structure

The rest of the thesis is structured as follows:

Chapter 2 reviews the literature focused on identity theft, knowledge management and corporate communications. The definitions of identity theft and current understanding of these concepts are evaluated. Next, knowledge management and its role in addressing and mitigating identity fraud are considered. Discussion of corporate communication practices support inter-organisational knowledge sharing activities. Research gap is identified with the discussion of the key research questions. The chapter concludes by proposing a need of the framework that helps understand online retailers' knowledge sharing practice.

Chapter 3 further extends the theories discussed in chapter 2. This chapter begins with an exploration of an appropriate theoretical framework useful to evaluate inter-organisational knowledge sharing process. Three frameworks are compared and contrasted and the components of the framework are synthesised. An extension of the framework in the security profession is proposed due to lack of empirical investigation in the online retail.

Chapter 4 concentrates on the methods applied. The philosophical underpinning of the research area and its theoretical stance is considered. This is followed by the design of case study, interview protocol, research instruments and the sampling strategy. The chapter concludes the field visits.

Chapter 5 presents the data obtained from various cases. It discusses background of the companies and their relevance to the study. Data from various cases is summarised and cross-case comparison is generated.

Chapter 6 discusses framework evaluation and extension. Answer to various key research questions is evaluated and summarised with key findings.

Chapter 7 concludes by discussing theoretical contribution. Key implications and recommendation are drawn. Challenges faced during this study are discussed to suggest future researchers about the promising research areas. The chapter concluded at the reflection.

Figure 1-1 illustrates structure and roadmap of the study.

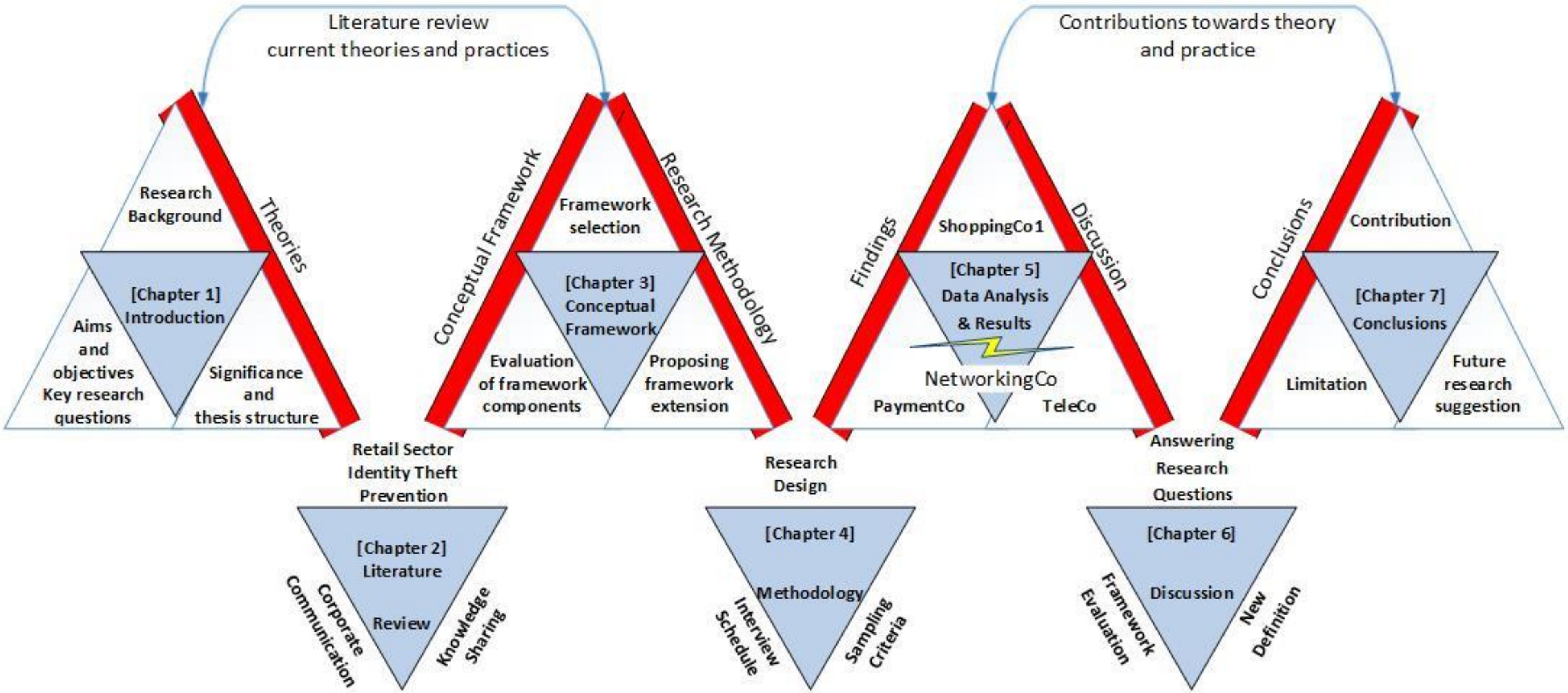


Figure 1-1 Organisational structure of key compoenents in knowledge sharing in relation to the thesis

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

This chapter reviews relevant literature involved in identity theft, knowledge management and corporate communication. The main aim is to evaluate inconsistencies, shortcomings, and contradictions in these broader research areas. The origin of the concepts and current understandings within the context of online retail is considered. Issue of identity theft prevention is discussed by arguing that knowledge management as a practice has received little attention to improve technicalities in security profession. Role of knowledge management to address and mitigate identity theft has been discussed. Next corporate communication methods that are commonly used to support inter-organisational knowledge sharing processes are addressed. The current knowledge sharing practices in the retail are evaluated. Research gap is addressed with design of the key research questions. The chapter concludes with a summary of the key findings.

2.2 Identity Theft – origins and current understanding

Identity theft is not a new crime, rather an evolution of an older crime enhanced with Internet (Newman and McNally, 2005). The first case of identity theft was discovered in the United States (US) when a mail theft in the late seventeenth century caused abuse of identity information of a member of the public (Jamieson *et al.*, 2012).

The question is what an identity is and how one steals it. An identity is not straightforward to define, because the concept is in infancy to take legal conceptual stance (Sullivan, 2009). It is rather complex and multifaceted in nature (Finch, 2003), and an integral to conceptualise a person within the society (Roberts, 2012). Identity was initially associated with regard to understand '*who are we'* from a life history (Schwartz, Luyckx and Vignoles, 2011, p. 2), '*what are we'* from biology (Newman and McNally, 2005, p. 39) and '*how are we'* from sociology (Lawler, 2008, p. 2). The first question considers how humans came into existence such as from Adam and Eve or the theory of evolution (Deane-Drummond, 2011). The second question reflects on their physical characteristics such as gender or race (Roberts, 2012). The third question focuses on social representation of the self to address how one relates to or is different from others (Finch, 2007; Lawler, 2008; Newman, 2004). Without digging deep into the first and second aspect of identity, this study evaluates how one relates to or is different from others, as this is associated with identity theft (Roberts, 2012; Finch, 2003).

Roots of an identity can be found in the late sixteenth century from Latin word 'Idem' which centres in the paradoxical meaning of 'sameness and uniqueness' (Lewis, 1890). To clarify this contradiction, sociological and psychological constructs is applied (Newman and McNally, 2005; Lawler, 2008). From a psychological perspective, Newman and McNally (2005, p. 39) define that when an individual refers to him or her, a *"person*" constitutes the same, when others refer to him or her constitutes a unique identity. From a sociological perspective, Lawler (2008, p. 2) defines that humans are identical, "*the same*", in all circumstances of life from birth to death, because they share common identities such as gender, authenticity, and nationality. However, uniqueness is considered as no one has the same lifestyle, not even the siblings or identical twins share all aspects of their life (Lawler, 2008). Thus, an identity provides an individual with a sense of self within society and a way of distinguishing themselves from others (Roberts, 2012).

A pertinent question is how an identity is stolen if it is associated with psychological or sociological constructs to understand someone's existence. Both represent intangible elements to perceive an individual. A misunderstanding of this terminology needs to be explored, as (Finch, 2007, p. 29) have noticed that "*the widespread acceptance of an imperfect understanding of the problem is potentially dangerous as it leaves individuals ill-equipped to protect themselves against victimisation*". Table 2-1 contains various identity theft definition as follows:

Table 2-1: Identity theft definitions

Definitions	***Authors***
"Knowingly transfers or uses, without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitute a violation of federal law, or that constitutes a felony under any applicable state or local law".	Newman and McNally, 2005, p. 1.
"Identity theft is the unlawful obtaining of identity documentation details (including personal identifying information used in customer not present situations or when customers interface with machines to authenticate, for instance personal identification numbers (PINs), passwords, key tokens or biometrics)".	Jamieson *et al.*, 2012, p. 383.
"Identity theft involves the theft of legal identity, manifest in identity tokens such as SSNs, documents or knowledge of information that identifies an individual".	Roberts, 2012, p. 22.

To clarify what is stolen when an identity is stolen, Finch (2007) has divided a person's identity into personal, social, and legal characters. A personal character is an internalised sense of self which constitutes how an individual perceives him or her in the past, present and future. Social identity is however opposite. Others perceive an individual in the social realm such as jolly, lively, arrogant, humble, hardworking and interactive. The third character of an identity is more important, because it legally differentiates an individual from others. Finch defines the legal identity as documentary accumulation identifier such as birth certificates, insurance numbers and credit reports (Finch, 2007, p. 30). Personal and social characters are intangible which self and others may perceive. However, legal character legally differentiates an individual from others. Therefore, an identity theft involves the theft of a legal identity (Finch, 2003).

Similar to Finch (2007), Roberts (2012) also has divided an individual's identity into three elements with a clearer perspective. Firstly, a biometric identity constitutes fingerprint and DNA profile. Biometric information might not be valuable to a fraudster, as they cannot use it to commit financial crimes; however, to an individual it is their identity. Secondly, an attributive identity is given to a baby at birth such as a 'name'. The third is biographical element refers to documentary accumulation that builds an individual over lifetime such as Social Security Numbers (SSNs) in the United States and National Insurance (NI) contributions in the United Kingdom. Biographical identities favour the fraudsters. An attributive identity is easy to assume, however, stealing biometric and biographical identities require obtaining identity tokens such as email addresses and passwords (Roberts, 2012, p. 22). The combination of email address and password help fraudsters to access into computer systems to collect key pieces of information that represent an individual.

Among the three definitions discussed (Table 2-1), Newman and MacNally's definition is useful as it shows what is stolen, what happens to an identity theft such as name or number that represents an individual are taken from them without their knowledge. This definition also suggests that criminals either use the same information or modify with other details slightly to perpetuate their online criminal activities. This theory, however, does not fully explain how identity theft is facilitated. The medium involved in supporting identity theft is considered in Jamieson *et al.*'s (2012) definition which suggests that an identity information is stolen when customers are not physically present at the time of shopping (i.e. online shopping), or when the customers interact with machines to download free online software or withdraw cash at cash machines.

This thesis is looking at the retailers who sell products and services through online channels. Therefore, the definition provided by Jamieson *et al.* (2012) is appropriate. It is specific to an online domain where the online transactional environment is involved. This definition brings into light many new elements such as PINs, passwords key token and biometrics. Are these identity details? Stealing email addresses incorporating user names and passwords is not actually an identity theft however, it lead to it. Roberts (2012) refers to these details as identity tokens. Some people misunderstand that identity theft is associated with the theft of card details such as numbers and codes used in online shopping. Card details are important, because it is like giving your wallet to someone when giving your card. However, Newman and MacNally (2005) argues that when a card detail is stolen is not same when stolen identity information. If the card is lost, a victim immediately can inform card-issuing authority to 'cease' usage and its misuse can immediately be observed through checking transactional information such as online statement. However, it is not the same with the loss of driving licence, social security number or health insurance number. These are the basic elements whereby an individual can be identified (Finch, 2003). Home address or birth date cannot be replicated and thus are unique. A house number belongs to an individual who owns or rents it. The same house number cannot be issued to a different person, unless it is a shared dwelling. Consequently, it may take a significant period to inform victims where these details were used fraudulently, until they receive correspondence from the company. Therefore, a financial loss is not actually the major loss as the personal details. An identity detail is thus valuable to an individual because it is not replicable (see Skjelsbaek, 2006).

Similar to identity detail fraudsters also favour Chip and PIN information. Chip and PIN are used to do shopping at the physical terminals such as point-of-sale (POS) system (Souvignet *et al.*, 2014), or withdrawing the cash using an Automatic Teller Machine. In POS transaction, one may need no personal information. However, placing an order online requires inserting card details such as card number, expiry date and Credit Verification Value (CVV) code. Placing an online order also requires customer's personal details including who are they and where do they live. Skimmers favour Chip and PIN information on the magnetic stripes, because it contains payment information (Souvignet *et al.*, 2014). However, the researchers failed to suggest reasons why do they favour data contained in the magnetic stripes and the PIN than identity information.

Khan (2015, p. 17) highlights another identity related fraud known as 'chargeback'. A chargeback fraud occurs when a consumers place an online order using their own card details. However, they request a refund from the issuing bank after receiving the goods. Merchants are accountable to refund regardless of steps taken to verify the transaction (Khan, 2015). This can be associated with first party fraud perpetrated by individuals using 'stealing' their own details (Cifas, 2015b, p. 7). This act is more associated with identity deception rather than identity theft. Identity theft is not same as identity deception. Figure 2-1 illustrates various terminologies used in identity theft and related crimes as follows:

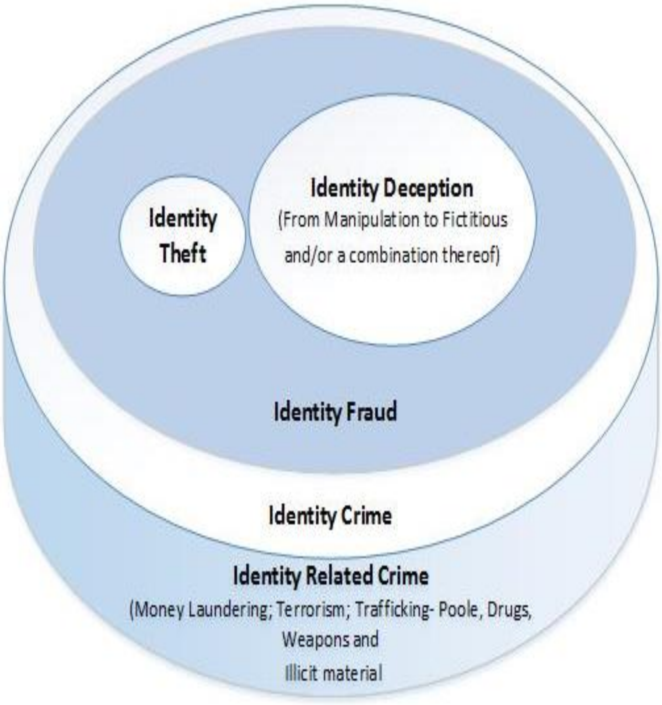

Identity Theft
Identity Deception
(From Manipulation to Fictitious and/or a combination thereof)
Identity Fraud
Identity Crime
Identity Related Crime
(Money Laundering; Terrorism; Trafficking- Poole, Drugs, Weapons and Illicit material

Figure 2-1: Conceptualisation of identity theft

Adapted from Jamieson *et al*. (2012)

Figure 2-1 shows that identity theft and identity deception are precursors of the identity fraud. Following definition modelled around identity fraud also clarifies this difference as follows:

> *"Identity fraud is the deliberate use of identity theft or identity deception details, for a financial gain or avoidance of loss to seek anonymity."* (Jamieson *et al.*, 2012, p. 383)

Researchers believe (Newman and McNally, 2005; Jamieson *et al.*, 2012; Sproule and Archer, 2007) that identity fraud is a generic term used interchangeably for identity theft and related crimes. Identity frauds are committed using stolen details or new fake identities. Stolen identities are associated with identity theft whereas creating fake identities are associated with identity deception. The former is related to abuse of a real person's identity, and the latter is associated with an alteration of the information through misrepresenting false or fake identities (Jamieson *et al.*, 2012; Sproule and Archer, 2007). More broadly, identity theft supports identity crimes and identity related crimes such as money laundering, terrorism and trafficking.

2.2.1 Identity Theft Channels

Two commonly used channels to support identity theft are physical and online. The criminals to steal identities in person at the site use physical channel. Cybercriminals use online channel to steal identities virtually.

Physical Channels

Physical is an easily approachable medium which does not involve any technological devices. However, this channel is risky, because perpetrator risk their presence (Fraud Advisory Panel, 2007). Paper mail, credit cards, and dumpster diving are the primary targets whereby identity details are commonly available (Roberts, 2012, p. 23). The first case of identity fraud caused due to a mail theft (Jamieson *et al.*, 2012). Financially motivated offenders go through the bins that contain financial letters (Newman, 2004; FTC, 2013). Opportunistic offenders take an advantage of lost wallets to victimise member of the public (Ruquet, 2012).

Shared accommodation and dwellings are common physical places whereby people stay together and share mailboxes. Opportunist fraudsters living in same occupied properties use this opportunity to access mailboxes (FTC, 2013). However, organised criminals target victims' bin in commercial and residential areas to obtain financial letter and other documents such as bank statements that identify a person (FTC, 2013). These methods are commonly known as dumpster diving and may involve colluding with a postal employee to assist in accessing financial information (Newman, 2004).

Although physical mediums are easily approachable, however are risky. Therefore, majority of the identity fraud are committed online channels (Cifas, 2015a) as explained below.

Online Channels

Online channels are 'playgrounds' of the fraudsters (Roberts, 2012, p. 21; Van Vlasselaer *et al.*, 2015, p. 38). Chapter 1 mentioned that technology plays a crucial role to facilitate identity thieves due to lesser chances of the person being caught (Ji *et al.*, 2007; Oluwu, 2009). Virtual communication facilitates perpetrator hide behind the computers. Cifas has reported approximately 82 per cent of identity frauds happened in the UK with online channels (Cifas, 2015a). Cybercriminals take an advantage of two common errors made by users and the businesses as follows.

Users' errors

Members of the public access online information inappropriately. Free online software applications such as online games and music attract common people. Accessing these applications is however dangerous. These applications automatically download malicious software that damage users' computer systems. Cifas (2014c) define malware as:

> *"Malware is malicious software that infects a victim's computer. It can capture private information that is stored on an individual's computer and send it to the fraudsters, who can use that information to impersonate the individual and commit fraud."*

User click bogus sites shared with either email attachments or click online application that infects computer. Cifas (2015a) provides its example of accessing JavaScript to support video players.

Users are also phished online to reveal their private information (Xu, 2012). Phishing is also a soft technique whereby fraudsters take advantage of human psychological weaknesses and tendencies of being unaware of the value of their information. It is rapidly growing threat to deceive an individual (Xu, 2012; Geeta, 2011). A fake website is designed that appears from a legitimate source such as users' financial institute, bank or insurance (FTC, 2013). Perpetrators also use phone excuses to deceive individuals to disclose their information (FTC, 2013). The fake advertisers use techniques such as fake group trips and airline reservations to reveal travellers' identity information (Travel Association, 2013). Association of British Travel Agents (ABTA) reported a worth million cases of suspecting travellers. The National Fraud Intelligence Bureau (NFIB) runs under the umbrellas of the City of London Police. NFIB has estimated approximately 1000 scams in the Britain which incurred £1.5 million only to holidaymakers (City of London Police, 2016).

Another common users' error is to submit online application that consists identity information. Thousands of job seekers submit resumes and curriculum vitae online that consists of substantial personal information (Sweeney, 2006).

Business errors

Businesses transform their functions from onsite to online (Turville, Yearwood and Miller, 2010; Lai, Li and Hsieh, 2012). This transformation supports staffs' mobility (Hunter, 2013); thus, employees can work from homes. As a result, day-to-day business activities are undertaken by accessing online information systems (Liefeld, 2013). Gartner reported more than 75 per cent of business applications and 50 per cent of critical operational data are accessed from the cloud. More than 2000, Chief Information Officers (CIO) worldwide participated in the Gartner's survey (Hunter, 2013). On one hand, advanced technology and Internet facilitated smooth business operations. On the other hand, however, it provides weak link to expose business information systems to a motivated criminal. Most of the businesses that has online presence collects and stores personally identifiable information from its customers, employees and collaborators (Geeta, 2011). There is on-going trend in business automation. Online business transaction has led to a large number of identity theft incidents (Lai, Li and Hsieh, 2012).

2.2.2 Identity Theft Consequences

Home Office Steering Committee calculated £1.7 billion cost incurred on the UK economy due to identity theft (Home Office, 2012). A similar impact found in the US which indicated $50 billion annual loss from identity frauds (Bindra, Shrivastava and Seth, 2012). A single identity fraud case victimises two parties. The first is an individual whose identity is stolen. The second is the organisation whose services are stolen (Newman and McNally, 2005; Newman, 2004). An individual whose identity is stolen may not bear financial loss (e.g. McKelvey, 2000; LoPucki, 2003). An individual however faces criminal investigation and bad credit ratings. Financial institutes bear the loss (e.g. McKelvey, 2000; LoPucki, 2003). Society however pays identity loss implicitly. Lai, Li and Hsieh (2012) have discovered that online businesses spend a considerable cost on intelligence to prevent identity frauds. Consequently, they increase prices on products and services (Wilhelm, 2004).

A company, however, loses a considerable amount if its reputation is damaged due to fraud news spread on the social media (Geeta, 2011). IBM's research group noticed that online businesses considered IT system failure as a major problem (IBM Global Technology Services, 2012). The companies now invest efforts on the reputation, because it is the key success driver regardless whether business involves physical or virtual transaction (Geeta, 2011). News of business frauds spread in public may cause reputational loss (Geeta, 2011). If the company were trustworthy, customers would like to buy its products and recommend them to others. Investors and potential employees want to be a part of it and communities will welcome its operations (IBM Global Technology Services, 2012). Consequently, businesses deal with identity frauds privately through using in-house intelligence systems. This is evident from Professional Security fraud report published on 17th February 2015, which states that:

> *"Companies are increasingly assessing the reputational cost to their brands of a public case against the cost of pursuing the perpetrators of the fraud through the courts. This is leading large numbers of cases being dealt with privately in-house and through alternative remedies."*
> (Professional Security, 2015)

2.2.3 Identity Theft Prevention Practices

To combat with online identity theft, corporations implement various countermeasures. These countermeasures may be divided into technical and strategic. The technical measures focus on enhancing technological practices such as dynamic password generators, SMS based one-time passwords, personal digital certification and electronic signature (Bose and Leung, 2013). Strategic measures involved human analytics to identify fraudulent cases (Ahmad, Maynard and Park, 2014; Wilhelm, 2004; Elyas *et al.*, 2015). This also involves attitude, norms, beliefs, behaviour, leadership and awareness (Flores, Antonsen and Ekstedt, 2014).

Technical measures are however considered as primary response, because the problem of identity theft is increased with the use of Internet and technology (Bose and Leung, 2013; Ahmad, Maynard and Park, 2014). This led to a number of technological developments including chip-and-PIN card system (Finch, 2011), the use of Secure Socket Layer (SSL) encryption for online transactions (Geeta, 2011), intrusion detection programs (Vrakas and Lambrinoudakis, 2013), and antivirus, firewall and data encryption systems (Roberts, 2012; VeriSign, 2012). However, identity thieves sneer at the security measures implements the companies. Regarding technical measures, Kevin Mitnick, a well-known American hacker states that:

> *"Companies spend millions of dollars on firewalls, encryption and secure access devices, and its money wasted, because none of these measures address the weakest link in the security chain."* (The Economist, 2002)

Criminals evolve to learn sophisticated attacks (Xu, 2012; Geeta, 2011). Retailers also need to evolve their technical abilities (Tamjidyamcholo *et al.*, 2013; Roberts, 2008). Strategic evaluation of security measures may help retailers in improving technicalities (Flores, Antonsen and Ekstedt, 2014; Ahmad, Maynard and Park, 2014; Tamjidyamcholo *et al.*, 2013; Elyas *et al.*, 2015; Kyoung-Joo, 2011), because strategy is:

> "*An art of deciding how to best utilise what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defence organisation's information infrastructure(s) against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective.*" (Park and Ruighaver, 2008, p. 27)

This definition suggests that strategy provides a comprehensive evaluation on the security measures that help decision makers to decide which construct is useful to prevent an attack. However, rather than focusing comprehensive evaluation, most researcher carried strategy by evaluating single construct. For instance, Glancy and Yadav (2011) have developed a computational model to help detect frauds; Knapp *et al.*, (2009) developed a framework that considers organisational policy only to help prevent online threats; Bhattacharyya *et al.*, (2011) considered data mining strategy only to overcome credit card frauds. Though there is limited empirical work on these measures, few studies are comprehensive (Ahmad, Maynard and Park, 2014; Wilhelm, 2004; Elyas *et al.*, 2015). These comprehensive studies are summarised in (Table 2-2).

In Wilhelm (2004), introduced fraud management lifecycle with eight stages to reduce an adverse impact of financial fraud experienced the businesses in the UK. These stages involve deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution. He tested his model in the industries such as retail, banking, credit or debit card issuing authorities, insurance companies and mortgages.

Table 2-2: Comprehensive frameworks in information security

Components	***Authors***
Deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution	Wilhelm, 2004, p. 15.
Prevention, deterrence, surveillance, detection, response, deception, perimeter defence, and compartmentalization	Ahmad, Maynard and Park, 2014, p. 364.
Organisational factors (governance, top management, culture), strategic factors (forensic policy, non-forensic stakeholders, forensic stakeholders and forensic training), infrastructure (technology and architecture), and forensic objectives (regulatory compliance, legal evidence management, forensic response, and business objectives)	Elyas *et al.*, 2015, p. 89.

Ahmad, Maynard and Park (2014) conducted a study a decade later with Korean organisations. They used nine controls such as prevention, deterrence, surveillance, detection, response, deception, perimeter defence, compartmentalisation and layering. These researchers empirically examined the businesses in software development, system integration, manufacturing, security consultancy and IT solutions. This third model mentioned was tested in the Australian organisations with law enforcement, consultancy, business and education (Elyas *et al.*, 2015). This model categorised factors of the framework into organisational, strategic and infrastructure to evaluate forensic readiness of the companies. Deterrence, prevention, policy are the common constructs mentioned in Table 2-2. Table 3-2 defines these constructs.

Deterrence is the first stage in fraud prevention life cycle which prevents fraud from its occurrence (Wilhelm, 2004). Offenders are informed about consequences for breaching company rules (Prabowo, 2011; Ahmad, Maynard and Park, 2014; Da Veiga and Eloff, 2010). A policy document is designed to define legal fines and actions for the staffs that fails to follow company rules such as sanction and certainty. For instance, Ahmad, Maynard & Park (2014, p. 360) have suggested that: "*One of the main foci of deterrence is in the security policy where deterrence has been used to specify the punishment of employees that fail to adhere to policy statement*". Doing so assists organisations to control employee behaviour (Da Veiga and Eloff, 2010).

Table 2-3: Strategic measures undertaken in information security

Components	***Purpose and example of activity***	***Literature***
Policy	A written set of general rules designed to guide the insider behaviour in the organisation through limiting the discretion of subordinates	Wilhelm, 2004; Knapp *et al.*, 2009; Knoppen, Christiaanse and Huysman, 2010; Elyas *et al.*, 2014
Deterrence	Inhibiting certainty for non-compliance of the policy in the organisation through card activation programs and fears of sanction such legal fines or prosecution	Ahmad, Maynard and Park, 2014; Wilhelm, 2004
Compartmentalisation	Dividing intended areas of attack into zones	Ahmad, Maynard and Park, 2014; Ahmad, Bosua and Scheepers, 2014
Surveillance	Systematic monitoring of security environment such as the use of Closed Circuit Television (CCTV) in the organisations	Ahmad, Maynard and Park, 2014; Elyas *et al.*, 2014; Marshall and Tompsett, 2005
Awareness or Trainings	Educating staff on their specific roles and responsibilities with respect to information security	Elyas *et al.*, 2014
Security culture	Design and implementation of shared beliefs and practices to guide the security culture among the staff	Elyas *et al.*, 2014
Regulatory compliance	Ability of an organisation to demonstrate adherence to law	Knoppen, Christiaanse and Huysman, 2010; Elyas *et al.*, 2014
Detection	Operation to uncover presence of fraud using statistical monitoring program	Ahmad, Maynard and Park, 2014; Wilhelm, 2004; Van Vlasselaer *et al.*, 2015; Glancy and Yadav, 2011
Analysis	Finding root cause analysis of suspected cases.	Wilhelm, 2004
Investigation or Evidence management	Operational strategy used to collect evidence to support legal proceedings.	Ahmad, Maynard and Park, 2014; Wilhelm, 2004; Elyas *et al.*, 2014
Prosecution or Response	Asset recovery and criminal restitution employing corrective actions against specific behaviour.	Ahmad, Maynard and Park, 2014; Wilhelm, 2004

Despite considerable effort on designing the security policies, organisations failed in controlling employees' harmful behaviour (Okeke, 2015; Vance, Siponen and Pahnila, 2012). This is evident from Cifas Internal Fraud Database (IFD) reported 4.3% increase in internal frauds whereby members of the staffs fraudulently accessed and sold consumers identity information (Cifas, 2015b, p. 35). One of the major reasons for this failure may be that organisations are not efficient to dictate policy to staffs. This is evident from security officials working in the Australian organisations that "*It should be made clear for employee what is appropriate and what is not. Also the consequences of* *noncompliance should be made clear"* (Elyas *et al.*, 2015, p. 77). Otherwise, policy will remain a paper tiger with no teeth (Knapp *et al.*, 2009, p. 500).

Controlling an external behaviour through policy is still in infancy. Companies offer online applications guide users' behaviour. For instance, Google recently has highlighted a privacy policy that covers information security. The policy states that Google will collect device identity, Internet Protocol (IP) addresses, cookies and current locations of the users for security reasons. Data is collected for the purposes of improving protection against online frauds and information misuse (visit https://www.google.co.uk/intl/en/policies/privacy/?fg=1).

Regulatory authorities such ass International Organisation for Standardisation (ISO) and Information Security Management Systems (ISMS) has designed a set of rules to help companies secure consumers' information. Organisation need to be compliant with these rules. These abilities assist an organisation to generate and retain accurate audit records in a prescribed manner (Elyas *et al.*, 2014).

Businesses also deploy systematic monitoring of the security environment. This is called surveillance. Surveillance is employed to support the investigation process (Wilhelm, 2004). Situational awareness of assets that adapt to rapidly changing circumstances is deployed (Ahmad, Maynard and Park, 2014). Marshall and Tompsett (2005) suggest that the installation of CCTV cameras is useful in monitoring critical premises and hence surveillance. This contributes to the digital forensic readiness of an organisation (Elyas *et al.*, 2014). Once a suspicious act is identified, legal evidences are collected to take corrective actions. This is called detection (Ahmad, Maynard and Park, 2014, p. 310). Detection can be preventative or reactive process (Wilhelm, 2004). Detection as a preventative process is applied to resist an attack such as by dropping a connection or blocking an IP address which seem fraudulent (Ahmad, Maynard and Park, 2014). Detection as reactive process supports to take legal actions against identity thieves (Wilhelm, 2004, p. 14). Suspects are either prosecuted or fined to recover the item lost (Ahmad, Maynard and Park, 2014, p. 360).

Compartmentalisation is another useful practice that divides information systems which is stored at different compartments. Researchers (Ahmad, Maynard and Park, 2014, p. 361) suggest that dividing an information system into several compartments may prevent an attacker's access to entire information system. If an attacker were able to overcome the defence of one zone, he or she would not be able to access other zones automatically.

Organisations arrange in-house security awareness programs that spread value of personal information among the staffs. This may help organisations from employee errors from business information system inappropriately (Roberts, 2012; Elyas *et al.*, 2015; Albrechtsen and Hovden, 2010). Albrechtsen and Hovden (2010) evaluated organisational workshop that improves information security awareness and have discovered that organisations run mainstream awareness program in a top-down approach. They use of formal presentations, leaflets and posters to spread value of the identity information. A key problem with these mediums is that they focus on a general audience. Elyas *et al*. (2015) have discovered that a general awareness program would be useful if every member in an organisation attends data preservation programs. However, staffs involved in the data protection and forensic investigations need specialised training programs that show how investigation tools and techniques are used. This system may help organisations to create and spread security culture.

The strategic and technical practices discussed provides compelling evidence of the continuous progress in the domain of information systems security. However, researchers have noticed that technical measures have progressed more effectively in robustness than the strategic (Flores, Antonsen and Ekstedt, 2014, p. 91). Ahmad, Maynard and Park (2014, p. 258) have reported that "*there has been little field-work conducted to determine…how these strategies are deployed".* Even though there are a number of studies evaluating the strategic practices in online information security, very few focus on online identity theft prevention (Okeke, 2015). An integrated approach and a detailed implementation of security practices that help to address and mitigate identity theft is also lacking. Many constructs in these studies need a fuller explanation. Elyas *et al*. (2015) identified a role of internal and external stakeholder and their participants discussed a number of shareholders including Chief Information Officer (CIOs), risk management team and human resource. The study, however, failed to discuss how these actors support one another in the fraud prevention process. Therefore, requires a comprehensive study to provide clarity of roles and responsibilities in the security profession. Wilhelm (2004, p.20) supports this view as:

> *"Since the lifecycle stages were presented as part of a clear organisational challenge, they could be evaluated in detail as supporting element as organisational redesign".*

Strategic practices discussed need more evaluation. One of the strategic aspects lacking an empirical investigation is the communication and knowledge sharing among various actors hired to ensure information security (Tamjidyamcholo *et al.*, 2013). Coping with identity theft independently could be costly and difficult (Kumar, Kumar and Grosbois, 2007). Organisation cannot prevent identity theft alone effectively (de Crespigny, 2012). They need to collaborate through sharing learning experiences. An inter-organisational knowledge sharing practice in the security profession may assist organisations in preventing online attacks. They can generate solutions of better quality through sharing their practices (Feledi and Fenz, 2012). This may also help them to avoid implementing same security wheel. However, little attention is placed on exploring knowledge sharing practice (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Feledi, Fenz and Lechner, 2013). Few studies consider this area discussed in Section 2.5.

2.3 Knowledge Management

What is knowledge; how security professionals can benefit from knowledge management? Management is a business function to organise and utilise business resources (Barney, 2000; Easterby-Smith, Thorpe and Jackson, 2012). In the past natural resources such as labour, soil and capital were only considered key drivers of the business operations. Modern society is however known as a 'knowledge society', whereby people who can apprehend ideas to provide abstract thinking are playing central role in the economy (Styhre, 2011). Tsoukas (2011, p. 455) considered late modernity as "*the age of theoria par excellence*". Therefore, success of organisations partially depend on how efficiently knowledge management activities are carried out (Jasimuddin, Connell and Klein, 2014).

A number of theories such as classical, human relations, critical, decision, work activity, competency and process are devised to help management function efficiently (Easterby-Smith, Thorpe and Jackson, 2012). These theories detail existing practices of companies, but also concentrates on what it needs to improve. These theories and key features are illustrated in Table 2-4.

Table 2-4: Management perspectives

Theory	***Dominancy***	***Key Features***	***Type***
Classical	1910-1950	Functional activities	Normative
Human Relations	1940-1970	Motivating people to change	Normative
Decision Theory	1950-1970	Optimising decision	Analytic
Work Activity	1970s	Focusing on what managers' do	Descriptive
Competencies	Before 1970s	Skills required for effective performance	Normative
Critical	1990s	Social construction and politics	Analytic
Process	2000s	Learning and strategizing	Analytic and Normative

(Adapted from Easterby-Smith, Thorpe and Jackson, 2012, p. 5)

Research in these management perspectives mentioned in Table 2-4 are continue conducted regardless of the chronological order (Easterby-Smith, Thorpe and Jackson, 2012). A classic theory advised management how to perform business activities efficiently. The present thesis rather than only giving advice, also seeks to understand how management deals identity theft with the help of knowledge sharing practice. Critical theorists concentrate on the effects of society and technology on organisational development (Easterby-Smith, Thorpe and Jackson, 2012, p. 30). The role of technology may help to understand learning experiences of the businesses. However, technology is not the only construct that this study seeks to understand. A human relational theory supports management to motivate employees by providing them with a complete information associated with business activities (Lopez and Esteves, 2013; Verčič, Verčič and Sriramesh, 2012). Process theory however leads to the idea of management as a process whereby learning is emphasised with the creation and management of organisational knowledge (Easterby-Smith, Thorpe and Jackson, 2012; Nonaka, 1994; Nonaka and Takeuchi, 1995). Process theory not only concentrates on how managers should perform, but also assist them with analytic reasoning. Process theory also helps to assess impact of some parts of the organisation (Easterby-Smith, Thorpe and Jackson, 2012, p. 5). Process theory is deemed evaluative to explore information security department in the whole retail business.

Knowledge management history

Knowledge and its study is as old as human history. Classical Greek period provides its roots in the study of philosophy and epistemology such as Plato and Aristotelian work (Tsoukas, 2011; Nonaka and Takeuchi, 1995; Davenport and Prusak, 1998). Initially knowledge was associated with finding the virtues of life, and was considered as self-knowledge (Tsoukas, 2011). It recently gains new emphasis of 'old-age' subject in the management studies that explores how organisation process and/or create new knowledge (Nonaka, 1994; Nonaka and Takeuchi, 1995; Nonaka, Von Krogh and Voelpel, 2006). This new field gains academic popularity from middle of the 1990 (Easterby-Smith and Lyles, 2011; Tsoukas, 2011), and further seeks to extend knowledge and its subjectivity of humans who create and utilise it (Nonaka *et al.*, 2014, p. 139).

Knowledge management activities are necessary in an organisation due dynamic environment. Rapid changes allow employees to process and create new knowledge (Nonaka, 1994). Captured peers' knowledge is helpful to other professionals (Styhre, 2011). The deployment of rapidly evolving technology requires adoptable staffs to learn quickly to accomplish day-to-day organisational tasks (IBM Global Technology Services, 2012). Officials depend on each other knowledge, as Davenport and Prusak (1998) highlighted that knowledge is driven from the mind at work. Capturing and disseminating of knowledge at work assists business operation smoothly (Hsiao, Tsai and Lee, 2012). Knowledge management can be viewed as structural organisational capital embedded in organisational routines and standard operating procedures (Davenport and Prusak, 1998). However, knowledge management is umbrella term that refers to managing knowledge-intensive activities (Gottschalk, 2005). These activities therefore involve capturing, disseminating, storing and leveraging knowledge to enhance organisational performance (Easterby-Smith and Lyles, 2011; Jasimuddin, Connell and Klein, 2014; Hayes, 2011). The study of knowledge management, therefore, broadly encompasses four major elements such as knowledge typology, knowledge creation, knowledge storage and retrieval and knowledge transfer.

Figure 2-2 navigation maps key themes and issues in knowledge management literature (Jasimuddin, Connell and Klein, 2014). These authors focused on intra-organisational knowledge transfer. They examined the high tech business organisation to determine the factors that influence knowledge dissemination in an organisation. This navigation map, however, is also useful in identifying research gap. The factors affecting inter-organisational knowledge sharing have yet to be investigated. This thesis considers filling this gap by evaluating inter-organisational knowledge sharing in the security profession. Exploring what is working and what does not seem to be providing benefit to online retailer with regards to the knowledge sharing that help to address and mitigate identity theft may extend knowledge in the inter-organisational knowledge sharing practice.

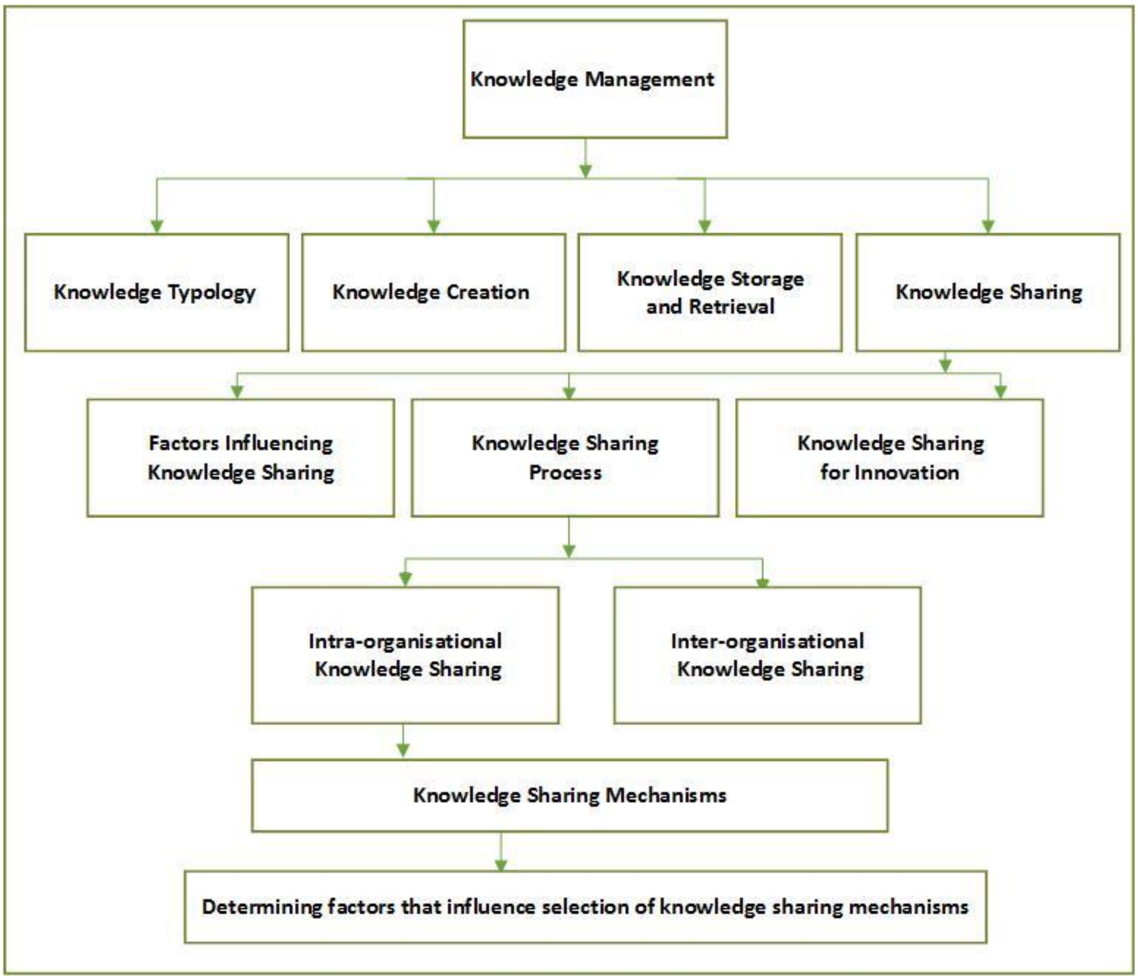

Knowledge Management
Knowledge Typology
Knowledge Creation
Knowledge Storage and Retrieval
Knowledge Sharing
Factors Influencing Knowledge Sharing
Knowledge Sharing Process
Knowledge Sharing for Innovation
Intra-organisational Knowledge Sharing
Inter-organisational Knowledge Sharing
Knowledge Sharing Mechanisms
Determining factors that influence selection of knowledge sharing mechanisms

Figure 2-2: Navigation map of knowledge management research

Adapted from Jasimudin, Connel and Klein (2014)

To explain various themes in a broad spectrum of the knowledge management literature, this study follows this navigation map described in the Figure 2-2. The diagram shows two major communication elements in the knowledge sharing process such as intra-organisational and inter-organisational. Since the focus of this thesis is inter-organisational knowledge sharing, it therefore concentrates on the constructs that address how different organisations communicate to explore information security knowledge. Chapter 3 explores how different inter-organisational knowledge sharing components are associated with each other to support the knowledge sharing process.

Knowledge management starts with strategic value in the knowledge. This then familiarises with the IT software such as databases and electronic conferencing to facilitate knowledge acquisition, sharing, storage, retrieval and utilisation (Easterby-Smith and Lyles, 2011). Hardly any industry makes full use of theoretical knowledge due to lack of resources (Tsoukas, 2011, p. 455). IT plays a central role to facilitate knowledge management activities (Hayes, 2011; Alavi and Denford, 2011; Alavi and Leidner, 2001). Therefore, a large body of literature in knowledge management focused on the IT applications that assists knowledge management in a company (Easterby-Smith, Crossan and Nicolini, 2000). However, there is ongoing debate whether knowledge management is achievable, because there is no clear distinction between information and knowledge (Wilson, 2002). Some researchers however use syntactic and semantic elements to clarify the differences (e.g. Nonaka, 1994; Alavi and Leidner, 2001).

Wilson (2002, p. 2) claims that, "…*what we know can never be managed*". The process of knowledge management only helps a mind to become manageable, thus the content of mind can be captured. He noted that people use data, information and knowledge synonymously:

> "…*National Electronic Library for Health uses the term 'Knowledge' because in the NHS information=data and a different term was needed."* (Wilson, 2002, p. 13)

There are various ways to express knowledge such as oral, written, graphic, gesture, and body language. However, these messages are not considered knowledge, but mere information, which a knowing mind can comprehend. As stated that knowledge is:

> *"…the mental processes of comprehension, understanding and learning that go on in the mid and only in mind, however much they involve interaction with the world outside the mind, and interaction with others."* (Wilson, 2002, p. 2)

Wilson's definition regarding knowledge can better be understood by considering the historical evolution over the time. Tsoukas (2011, p. 454) suggests that it may be necessary to participate and exercise the mind in a larger collective, however, so that is not occupied only in the values, but also in the abstraction, general principals and ability to obtain results. Similarly, Brandi and Elkjaer (2011) contend that learning is not restricted to take place inside an individual's mind but also in a process of participation and interaction with others. Therefore, it is suggested that information is a flow of messages, however, when we anchor that very flow into actions then it becomes knowledge (Nonaka, 1994).

Researchers including (Jasimuddin, Connell and Klein, 2014; Nonaka, 1994; Alavi and Leidner, 2001), stress that information is an important tool that supports knowledge creation. Information draws from the 'raw data'. Data, information and knowledge are related but not same, as Davenport and Prusak (1998, p. 1) put that "*we can understand knowledge best with reference to them [data and information]*". They provide an example using a transactional data that "*when [a] customer goes to gas station and fills the tank of his car, that transaction can be partly described through the data such as when he purchases, how many gasolines he bought, how much he paid*" (Davenport and Prusak, 1998, p. 2). Similarly, a telephone bill is calculated using a time duration and distance rather than what has been spoken (Nonaka, 1994).

Similar to data, information is also measured without considering meaning and value. This reflects Nonaka *et al*. (2014, p. 139) that "*knowledge is information in context and once we add context we add tacitness*". These are semantic elements whereby individuals consider conveying meaning embedded in the contextual details to constitute the knowledge (Nonaka *et al.*, 2014, p. 16). Distinguishing information from knowledge is often difficult and confusing when involves IT. Although IT strongly influences the message, however it is a medium, not the message (Davenport and Prusak, 1998, p. 2). The thing delivered is more important than the delivery vehicle. This view is similar to Nonaka (1994, p. 16) that information is an important tool that facilitates knowledge creation. They thus suggest that IT and information are the vehicles that help to develop and to organise the knowledge.

To evaluate knowledge using traditional epistemology, Nonaka (1994) found that it was previously considered static and nonhuman. He believed that knowledge was part of aspiration of truth "*justified true beliefs*" (p.15). However, he prefers to value the believing nature of the knowledge than justified nature. The present research evaluates knowledge from a communication perspective to assess how different organisations interact to share identity theft knowledge. Therefore, Nonaka's definition may not be appropriate. Organisations may need some elements of justification rather than belief. When different organisations are involved, require reasons. Individuals' belief probably natural and direct (Nonaka, Von Krogh and Voelpel, 2006, p. 1183), as Moran (2006) suggests that "*getting told and being believed*" (p.1). However, it is not easy for an individual to persuade someone by being told and believed (Simpson (2013a, p. 305). Within an organisation, this is the gist of synthesising new, practical, useful, valid and important knowledge added to existing knowledge base which makes justification hard (Nonaka, Von Krogh and Voelpel, 2006, p. 1183). From a Resource Based View (RBV) of the firm knowledge can be defined as:

> *"Knowledge is a fluid mix of framed experience, values, contextual information and expert insight that provides a framework for evaluating and incorporating new experiences and information. It originates and is applied in the mind of the knower. In organization it is often becomes embedded not only in documents or repositories, but also in organizational routines, processes, practices and norms."* (Davenport and Prusak, 1998: p. 5)

Knowledge in this definition is viewed as non-simplistic that combines fluid actions. This also involves formally constructed elements such as documents and repositories. Therefore, it is hard to capture and share knowledge with others (Davenport and Prusak, 1998). Capturing and sharing of domain specific knowledge may not require many efforts, because it engages similar patterns of work and standards for judgement (Hayes, 2011, p. 86). Domain specific knowledge refers to knowledge acquired through a commonly enacted body of competence and expertise (Styhre, 2011, p. 30). This thesis specifically looks at domain specific knowledge in the domain of information security to assess how peers help address and mitigate identity theft through sharing learning experiences. Therefore, it would be useful to consider how shared sense and standard of judgement is used to understand similar patterns of work. This study therefore adopts the definition provided by Davenport and Prusak (1998) to explore how security knowledge is created and shared in the online retail sector. This definition brings into light two different types of knowledge such as fluid mixture of experiences and organisational repositories.

2.3.1 Knowledge Typology

Organisational knowledge is a philosophical stance to understand, and conceptualise the nature of knowledge organisations holds in their possession (Easterby-Smith and Lyles, 2011). Researchers exploring knowledge typologies either distinguish between tacit or explicit (Easterby-Smith and Lyles, 2011; Jasimuddin, Connell and Klein, 2014; Jasimuddin, Connell and Klein, 2005). This understanding help to address value knowledge holds to benefit the business.

Michael Polanyi, a philosophical figure, brought researchers attention to two types of knowledge. Firstly, knowledge is referred to as an objective entity, where a seeker relies on theories for an understanding (Polanyi, 2003, p. 4). This is known as theoretical knowledge. Secondly, knowledge is viewed as a personal quality which need immediate sensory experiences for comprehension (Polanyi, 2003, p. 4). This is referred to as a practical knowledge. These two types are widely known as explicit and tacit knowledge (Davenport and Prusak, 1998; Alavi and Leidner, 2001; Polanyi, 1966). Former is based on theoretical comprehension and the latter requires practicality. The former carries codified language, and is communicated readily via online mechanisms. However, the latter is embedded in practice, therefore, requires the knowledge holder to clarify what they do.

Geography has influenced how researchers perceive knowledge scrutiny. The traditional western world viewed knowledge systematic and formal (Styhre, 2011). This knowledge is acquired through education and reading from books, newspapers, repositories and manuals (Awad and Ghaziri, 2007). The importance of this knowledge in the modern organisations is provided as follows:

> "*The increasing decontextualisation of knowledge in the modern age has led to theoretical (or codified) knowledge acquiring a central place in functioning of modern (especially late modern) societies*" (Tsoukas, 2011, p. 454).

However, few researchers omit the value gained from explicit knowledge as Sveiby (2009) states that:

> "*I do not believe much in lectures as means of transferring knowledge; I prefer experiential learning*".

In the Eastern countries, researchers such as Nonaka and his associates bring tacit knowledge to substantial awareness (Nonaka, 1994; Nonaka and Takeuchi, 1995; Takeuchi and Shibata, 2006). Nonaka (1994, p. 16) states that knowledge expressed in words and numbers represent the "*tip of iceberg*". Nonaka's work is based on the statement of Michael Polanyi (1966, p. 4) that "…*we can know more than we can tell*". Polanyi believed that most knowledge people acquire implicitly during schools, work and life experiences. People are even not fully aware of possession of this knowledge. This is knowledge is an important feature of organisation that underlies in skilful actions (Tsoukas, 2011). Therefore, sharing tacit requires it to be contextualised. It is also difficult for knowledge holder to clearly what they do (Polanyi, 1966). Then why researchers claim that IT – a virtual communication channel helps to share tacit knowledge (Alavi and Denford, 2011; Panahi, Watson and Partridge, 2013; Panahi, Watson and Partridge, 2015). May be, the synthesis of tacit and explicit knowledge such as *phronesis* (Figure 2-3) is able to communicate what officials do. Nonaka *et al*. (2014, p. 139) believe that phronesis drives through the interaction of tacit and explicit as illustrated in the triad model in Figure 2–3.

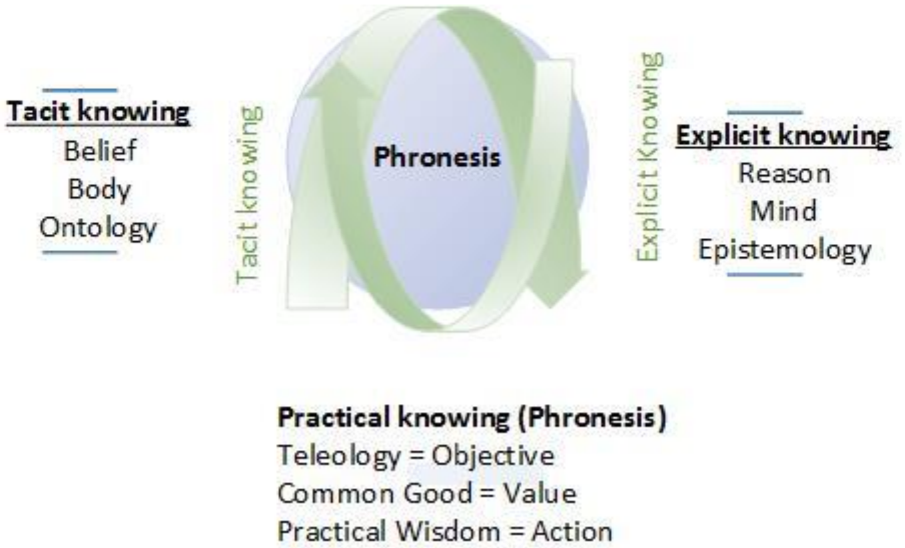


Figure 2-3: Spiral of knowledge types

Adapted from Nonaka *et al*. (2014)

Greek scholar Aristotle coined phronesis which means "*practical wisdom*". Tsoukas (2011) recently used phronesis in his argumentative study to Nonaka's knowledge conversion model discussed in the knowledge creation theory below.

2.3.2 Knowledge Creation Theory

Nonaka, Von Krogh and Voelpel (2006, p. 1179) define organisational knowledge creation theory as:

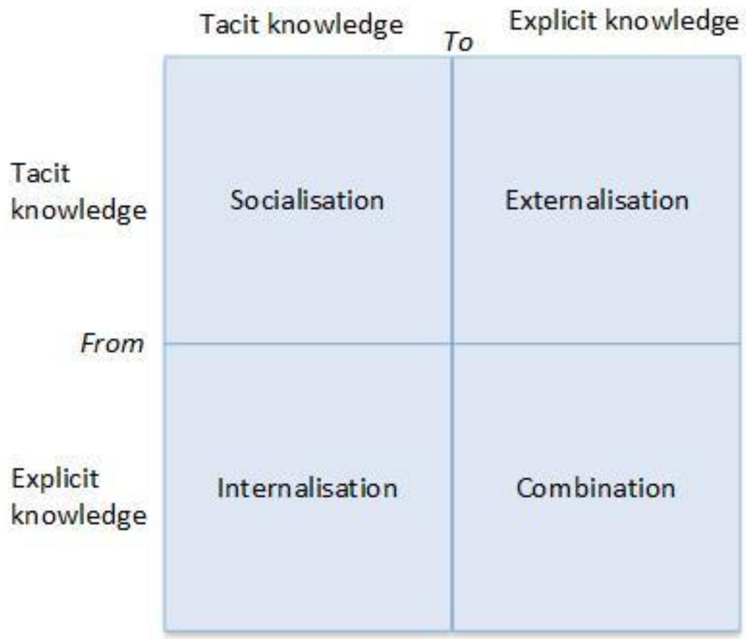
> "*The process of making available and amplifying knowledge created by individual as well as crystallising and connecting it with an organisation's knowledge systems".*

Whatever individuals acquire during a professional career can benefit their colleagues and the organisations. This is an important domain to assess how organisations collects and records knowledge from their employees (Nonaka *et al.*, 2014; Styhre, 2011). An organisation's knowledge creation theory encompasses epistemology and conversion. The former is associated with the act of knowing where special attention is given to the knowledge validity and limitations (Nonaka, 1994). The latter provides an insight to understand how official's subjective knowledge is connected to, and synthesised with others knowledge (Nonaka and Takeuchi, 1995). Nonaka *et al.* (2014) believed that innovation emerges with spiralling continuity and conversion between two types of knowledge discussed in previous section. This is reflected as follows:

> "*When an individual's tacit knowledge is shared with another person it becomes explicit knowledge, and when this is merged with other explicit knowledge it becomes new explicit knowledge, which in turn can then be converted into the tacit knowledge of an (other or the same) individual and thus link with the subsequent conversion process.*"
> (Nonaka *et al.*, 2014, p. 139)

The spiralling is extended from Nonaka's (1994, p. 19) previous work which suggests SECI, a model that reflects an organisation's knowledge creation. SECI stands for Socialisation, Externalisation, Combination and Internalisation. This model represents four modes of conversion to assist how organisational knowledge creation theory works in the workplace. This model is illustrated in figure 2-4.

For many researchers (Nonaka *et al.*, 2014; Easterby-Smith, Lyles and Tsang, 2008) knowledge creation process is context dependant. The context is '*Ba*' which stands for '*space of emerging relationships*' (Nonaka, Von Krogh and Voelpel, 2006, p. 1184). There are four emerging spaces of relationships such as originating, interacting, exercising and cyber.



From \ To	Tacit knowledge	Explicit knowledge
Tacit knowledge	Socialisation	Externalisation
Explicit knowledge	Internalisation	Combination

Figure 2-4: SECI model of knowledge conversion

Adapted from Nonaka (1994)

Figure 2–4 shows that conversion from tacit to tacit is achieved using a socialisation where an *originating Ba* may be useful to provide a space for face-to-face interaction. Thus, a new knowledge is created with the help of language, observation, imitation and practice (Nonaka, Von Krogh and Voelpel, 2006). Online real-time meetings, synchronous communication, chat, online community of practice and social media are common digital mechanisms that support socialisation process (Panahi, Watson and Partridge, 2013). Offline mechanisms such as team meetings, interpersonal interaction, apprenticeship, participation and observation also supports socialisation (Panahi, Watson and Partridge, 2013).

The next box at the top right in Figure 2-4 is useful to support knowledge exploitation whereby a newly gained external knowledge is converted into explicit to distribute with others. This process represents knowledge externalisation. Offline mechanisms such as dialog with teams, answering questions, storytelling, metaphors and analogies assist externalisation (Panahi, Watson and Partridge, 2013). The digital mechanisms involve blog, wikis, discussion forums and video conferencing (Panahi, Watson and Partridge, 2013).

The bottom-left box represents internalisation whereby an explicit knowledge is converted into tacit. A training activity is an example of this conversion. However, a trainer can be an instructor or colleague within the organisation. Commonly used offline mechanisms that support internalisation are learning by doing, learning from books, reports, presentations and lectures, whereas online mechanisms used are visualisation, video/audio presentations, online learning, email and web page (Panahi, Watson and Partridge, 2013).

The box in bottom-right is a combination process that represents conversions from explicit to explicit. Offline mechanisms that support this combination include books, papers, reports, presentations and indexes (Panahi, Watson and Partridge, 2013). Online mechanisms include various types of technologies such as text searches, documents, categories, blogs, wikis, and Rich Site Summary (RSS) feeds. In a cyber relationship a virtual space is created where thousands of professional can interact using medium such as Information and Communication Technology (ICT) (Nonaka, Von Krogh and Voelpel, 2006). Wikipedia is an example where users are provided an option to edit and add knowledge stored previously.

Organisational knowledge creation theory using SECI model has been debated in the research for many years. This is evidenced as follows:

> "*Aspects of tacit knowledge may be articulated, which, however, is not the same as converted or translate"* (Tsoukas, 2011, p. 456); "*…their potential lies in the tacit knowledge brought to their use by both their producers and their users"* (Ribeiro and Collins, 2007, p. 1430).

Accessing tacit knowledge requires both actions and retrospect. Therefore, seeing this knowledge in the conversion model is misleading. Even though explicit seems to be the easiest form of knowledge to articulate, it also underlies certain tacit elements which cannot be transformed completely. For instance, the transformation of manuals and books carry meaning that is provided by the author (Ribeiro and Collins, 2007, p. 1430). Collins (2001) accepts that a formalised theory based on pure mathematics cannot completely transform, as this requires application and development based on the skills of mathematicians. Therefore, seeing tacit on the conversion model may be argumentative.

These authors may be correct, because organisational knowledge creation theory was developed on the experiments from bread making machine. Nonaka and Takeuchi (1995) reflected on transferring Master backer's tacit knowledge into explicit, to transform a bread-making process. Ribeiro and Collins (2007) replicated the study to test theory in the European context. They have explored bread-making process particularly from tacit to explicit conversion. However, their results produced contradictions, because machine failed to learn completely the skills from a Master Baker. They have found that machine was useful to reduce human efforts in the backing process. However, the analytical measures including the choice of flour and amount of yeast required human skills. Therefore, they conclude that Nonaka and Tackeuchi selection of the case was wrong to evaluate knowledge creation theory (Ribeiro and Collins, 2007, p. 1418).

Tsoukas (2011), Ribeiro and Collins (2007) and Styhre (2004) noticed that tacit knowledge may lose its value, unless the organisation which holds it, replicates it into explicit. Therefore, they argue that tacit knowledge has either been widely "*misunderstood*", "*not yet articulated"* or "*a weak form of explicit knowledge"*, (Tsoukas, 2011, p. 455; Styhre, 2004, p. 186; Tsoukas, 2005, p. 154). Tacit knowledge occupies intellectual and corporeal capabilities that individuals cannot 'fully' articulate or codify (Styhre, 2004, p. 178).

In response to these arguments, Nonaka *et al.* (2014) recent study suggest that knowledge exploration and exploitation requires conversion. Because, although tacit and explicit are dissimilar, however, lie in the continuum. Arguably this is correct, because there will remain no value from exploring knowledge from other organisations if it is not exploited and/or used in the company (Easterby-Smith, Lyles and Tsang, 2008). This requires converting tacit knowledge into explicit, because high elements of tacit are commonly found in knowledge exploration process whereas explicit in knowledge exploitation process (Nonaka *et al.*, 2014, p. 140).

Knowledge articulation may be weak when tacit knowledge is converted into explicit. However, the domain specific knowledge holders may not lose complete value in the knowledge conversion process, if they share similar patterns of work. People working in the same profession are able to share and understand what another peer do. Organisation, therefore, may consider enhancing skills rather than focusing on gaining complete value from tacit knowledge. Therefore, rather than arguing who to support with regards to seeing tacit knowledge in the conversion model, this study focuses on how knowledge exploration and exploitation is achieved through the synthesis and conversion of tacit and explicit knowledge. This practice may help an organisation to understand extent to which knowledge exploration and exploitation works in the security profession to prevent identity theft. Michael Polanyi also supported this assumption by stating that:

> *"…theory being paced like a screen between our senses and the things of which our sense otherwise would have gained a more immediate impression. We would rely increasingly on theoretical guidance for the interpretation of our experience, and would correspondingly reduce the status of our raw impression to that of dubious and possibly misleading appearances."* (Polanyi, 1962, p. 3)

Polanyi's statement suggests that knowledge of tacit and explicit are necessary for a clearer understanding. Explicit knowledge helps improved understanding of the tacit knowledge. This study pays attention to how knowledge exploration and exploitation helps knowledge integration and use. The triad model discussed previously (Figure 2–3) may help synthesis to a practical wisdom (Nonaka *et al.*, 2014). This thesis concentrates on the security profession only, therefore may be no difficulty in articulating knowledge from the same domain. Synthesis of tacit and explicit may deemed appropriate for a fluid mix of knowledge.

2.3.3 Knowledge Storage and Retrieval

Almeida, Hohberger and Parada (2011, p. 383) discussed two steps to gain and use an external knowledge. Firstly, source knowledge from other organisations. Secondly, integrate knowledge with firm's existing knowledge base. Former requires interacting with external sources through attending networking conferences or collaborating with past colleagues (Easterby-Smith, Lyles and Tsang, 2008). Latter constitutes re-combining knowledge gained from several sources into an existing body of knowledge within the organisation (Nonaka *et al.*, 2014). Both source and integration help improve organisational memory (Klein, Connell and Jasimuddin, 2007). Klein, Connel and Jasimuddin (2007) believed that there is a strong relationship between organisational learning and organisational memory, since one leads to the other.

Knowledge storage helps combining new knowledge into company's existing knowledge base. Almeida, Hohberger, and Parada (2011, p. 396) have found that company's central system facilitates internal communication by locating knowledge at one place instead of numerous distributed locations. A centrally located knowledge base helps other colleagues in knowledge utilisation. However, professional further require frequent interaction with each other across extended period of time to clarify what they share (Almeida, Hohberger and Parada, 2011). Theories on internal communication that support knowledge integration are extended in (Section 3.3.2) to understand knowledge storage and use. The characteristics of officials who help knowledge exploration and integration process are further discussed in (Section 3.3.1).

2.3.4 Knowledge Sharing

Individuals hold ideas, creativity and innovative capacity. However, these ideas are not developed in isolation, but are always the result of collaborative efforts (Styhre, 2011). Nonaka (1994, p. 15) puts this view as "*although ideas are formed in the mind of individuals, interaction between individuals typically plays a critical role in the developing such ideas*". Although, there appears to be a difference in opinion regarding the data, information and knowledge discussed previously (Nonaka and Takeuchi, 1995; Wilson, 2002), however, both researchers come to a common ground that an individual requires an interaction with the world to enhance the idea. People see the solutions of the problems differently. In the collaboration, they seek different aspects of the same problem (Tiwana, 2000). Thus, communication among the professionals not only supports to develop new knowledge but also enriches the older one, as Davenport and Prusak (1998: 17) suggest that: "*ideas breed new ideas and shared knowledge stays with the giver while it enriches the receiver*". Usoro and Majewski (2011) agree stating that knowledge tends to increase when shared and utilised. Success of knowledge management depends on knowledge sharing and collaborative efforts taken by the knowledge holders. Therefore, it is useful to distinguish various terminologies used in the knowledge management that refer to knowledge sharing practice.

Researchers worldwide use knowledge transfer more often than knowledge sharing or exchange (Wang and Noe, 2010; Matthews and Shulman, 2000; Ghaznavi *et al.*, 2013). Difference in these terminologies can be explained through using modes of communication, flow of information, reciprocity, knowledge application and use (Ghaznavi *et al.*, 2013; see, Ghaznavi *et al.*, 2011; Boyd, Ragdell and Oppenheim, 2007). These differences are illustrated in Figure 2–5.

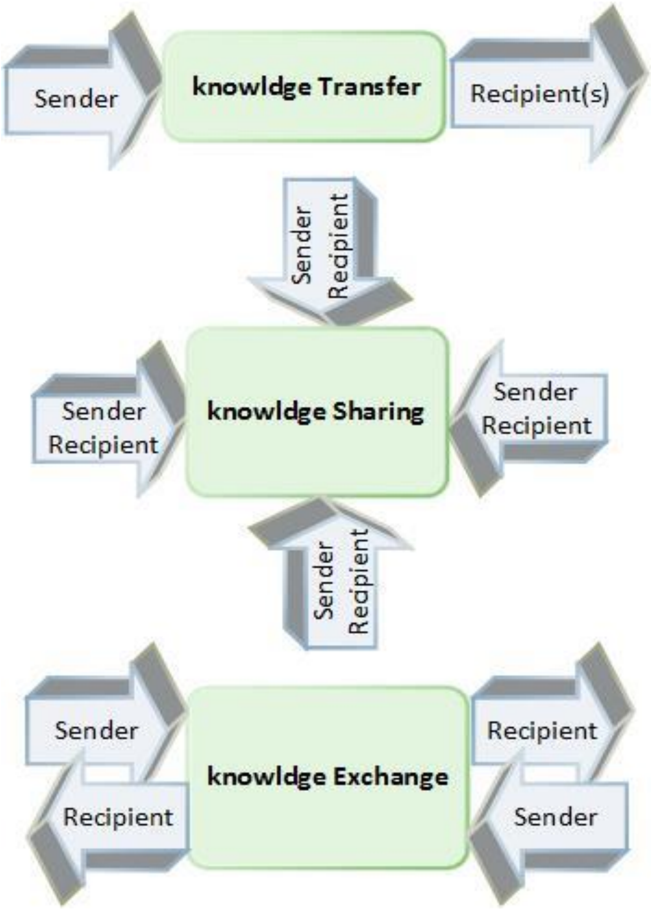


Figure 2-5: The knowledge flows
(Adapted from Boyd, Rogdell and Oppenheim, 2007)

Figure 2–5 shows that knowledge transfer is a unidirectional process, whereby knowledge flows from a sender to the recipient(s). This is a non-reciprocal process with only one knowledge distributor to many knowledge seekers (Boyd, Ragdell and Oppenheim, 2007). Training is its common example. Knowledge recipient not only gains new knowledge but also applies it to a different context (Wang and Noe, 2010). Knowledge transfer is different from knowledge sharing and exchange, because it pays attention on units, divisions and organisations rather than on individuals' interaction (Wang and Noe, 2010). This thesis aims to explore security officials' interaction to learn from peers in other businesses; therefore, knowledge transfer process may not be useful in this context. However, an element that suggests how recipient apply new knowledge into a different context deemed useful to understand how gained knowledge is valued.

Knowledge exchange is a reciprocal process, whereby an owner of the knowledge also wants knowledge of equal value (Ghaznavi *et al.*, 2013). This process involves one sender and one recipient. This practice is normally found in formal contracts (Boyd, Ragdell and Oppenheim, 2007). Liu, Ji and Mookherjee's (2011) study conducted in information security domain evaluates contractual governance between two organisations. Since, the contractual governance is involved in knowledge exchange; communication may be limited to senior management only. However, senior management does not necessarily perform actual work to ensure information security (Ahmad, Maynard and Park, 2014). They are mostly engaged in decision-making process for sound business decisions (Feledi, Fenz and Lechner, 2013). Security professionals may improve their technicalities by sharing ‘practical knowledge’ (Tsoukas, 2011). Senior management may not provide practical wisdom. Knowledge exchange may be limited to access one type of knowledge (Sammarra and Biggiero, 2008, p. 811). Information security officials’ skills are diverse and may require access to multiple types of knowledge. Thus, it requires a wider channel to support access to different types of knowledge.

Knowledge sharing is not limited to number of people. This practice may be reciprocal or non-reciprocal. Figure 2–5 shows that knowledge sharing is a multi-directional process that facilitates a number of individuals to interact with one another. An owner of the knowledge can also be a recipient (Boyd, Ragdell and Oppenheim, 2007). A networking activity such as conference may be a good example of this process. As stated:

> *“Knowledge sharing is a social practice that is both contingent on local conditions and histories and shaped and influenced by professional ideologies and professional skills.”* (Styhre, 2011: 52)

Since, this thesis is looking at how different knowledge actors working in the security profession explores knowledge from each other, thus knowledge sharing practice is favoured than knowledge transfer or exchange. This thesis however also considers extent to which organisations are willing to share fraud related knowledge with one another. Therefore, some elements of knowledge exchange are also favoured to explore contractual governance used in the partnership.

Knowledge sharing practice consists of many elements such as communication practices, instituted routines, human capital, technology and organisational relationships. Communication is prerequisite to knowledge sharing regardless whether it is printed or verbal, formal or informal, and face-to-face or digital (Jasimuddin, Connell and Klein, 2014; Alavi and Denford, 2011). Choice of the communication strategy depends on need and the relationship among knowledge holders. Figure 2–2 have illustrated two communication processes used to share knowledge. The first concentrates on internal communication where members of same organisation share knowledge with one another (intra-organisational knowledge sharing). The second considered how peers from different organisations communicate (inter-organisational knowledge sharing). The former facilitates knowledge exploitation within staffs and latter requires external communication to explore knowledge from other organisations. Since this thesis aims to explore how peers learn from other peers working in different organisations, therefore, theories that address how and why corporate employees communicate with one another is favoured.

2.4 Corporate Communication

Communication is an everyday activity; however, corporations are the hub where people communicate on a daily basis (Littlejohn and Foss, 2008; van Riel and Fombrun, 2007). Corporate communication is the basis for the survival in all business activities (van Woerkum and Aarts, 2008). Due to communication, organisations acquire primary resources such as capital, labour and raw material. These primary resources help to generate secondary resources such as legitimacy and reputation (van Riel and Fombrun, 2007, p. 1). This in turn helps companies to earn. Many researchers state that knowledge sharing and communication are symbiotic, because one leads to the other (Nonaka *et al.*, 2014; Jasimuddin, Connell and Klein, 2014). Eventually, this seems true because the word corporate stems from the Latin word 'corporare' which means '*forming into a body'*. Communication came from 'communicare' which means '*to share'*. Both knowledge and networks thus are crucial to an organisation (van Wijk, van den Bosch and Volberda, 2011, p. 478).

Littlejohn and Foss (2011, p. 5) while discussing communication theory have identified that communication theory was initially borrowed from information theory, social psychology theory and linguistics theory. Social psychologists have used communication theory to understand human behaviour, whereas sociologists concentrate to understand importance of the society. The communication theory gained attention after World War I. Organisational communication theory, however, developed more recently in the middle of the twentieth century. One definition that fits all types of communication would be misleading, as Littlejohn and Foss (2011, p. 5) have found that "*different sorts of investigation require separate, even contradictory, definitions of communication"*. A definition thus requires being specific enough to fit in the context being investigated.

Since this study considers communication among security officials in the online retail, theories that address how corporates communicate with one another are favoured and explained in Table (2-5).

Table 2-5: Corporate communications theories

Definitions	***Authors***
"Corporate communication is a management function that offers a framework for the effective coordination of all internal and external communication with the overall purpose of establishing and maintaining favourable reputation with stakeholder groups upon which the organisation is dependant."	Cornelissen, 2014, p. 5
"We define an organisation's communication system as the multiple tactical and strategic media it relies on to communicate with its stakeholders, as well as the message content it chooses to diffuse through that media"	van Riel and Fombrun, 2007, p. 2

Cornelissen's definition (Table 2-5) has two shortcomings. It is generic and such an element suggests that the 'overall purpose' of communication is to maintain reputation and image. Reputation and image are essential elements for any type of business, because it helps to attract consumers, obtain licence from government authorities, and to find potential investors (van Woerkum and Aarts, 2008). Although corporate communication influences its participants and observers about company and its operation, however, not all communications in an organisation are work related; neither is relevant to fulfilling organisational objectives (van Riel and Fombrun, 2007). This thesis, however, considers reputation and image, because these elements support building positive relationships (Fieseler and Ranzini, 2015, p. 500-517; Simpson, 2011, p. 32). Creating an alignment with external groups requires an understanding of their beliefs about the organisation. Thus, requires better reputation and impression to explore external knowledge (van Riel, 2013).

Between the two definitions discussed (Table 2-5), van Riel and Fombrun's definition is useful, because it also covers media that supports knowledge sharing, and concentrates on the content being communicated. The content aspect of the definition such as 'knowledge' is discussed previously (Section 2.3). However, it is not the knowledge only that leads organisations to communicate. Following model shows clearly how its environment influences organisations.

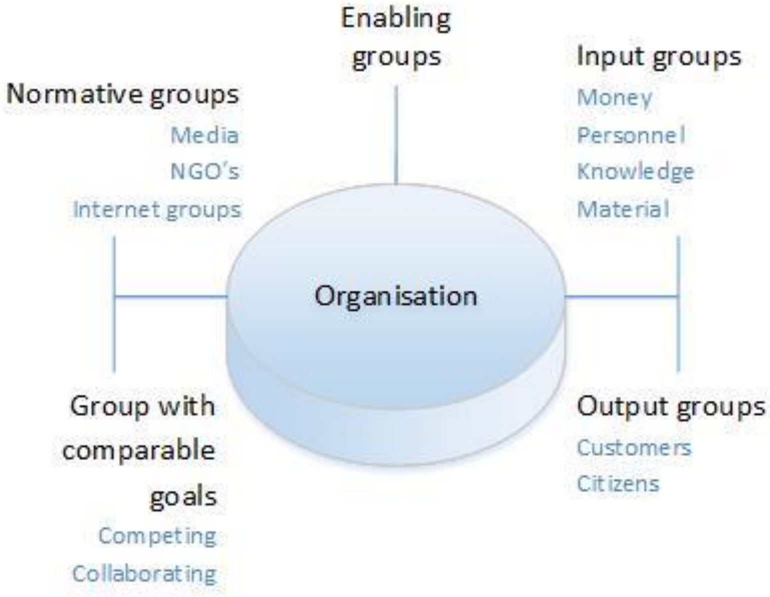


Figure 2-6: An organisation and its environment

Adapted from van Woerkum and Aarts (2008)

In Figure 2–6, van Woerkum and Aarts have shown the basic needs of an organisation to communicate with others. They have believed that an internal group such as employees constitute an organisation. The employees are crucial stakeholders that require frequent communication to provide a complete knowledge to accomplish day-to-day specialised tasks (Cornelissen, 2014). Argenti (2013, p. viii) reports that officials often perform different activities at the time. A coherent communication keeps track of the knowledge acquired by thousands of employees. Internal communication is a constant activity that utilises several mechanisms such as informal chat and organised meetings (Welch and Jackson, 2007). To report importance of internal communication, Easterby-Smith, Lyles and Tsang (2008) suggest that exploring external knowledge is wastage, if management do not communicate with internal staff. If management keeps information from staff, they keep their ideas (Argenti, 2013). Internal communication practice thus requires effective tools. The theory on internal corporate communication is extended (Section 3.3.2) to evaluate the abilities of an organisation to support internal knowledge dissemination practice.

Figure 2–6 shows five important external groups necessary for external communication. An enabling group represents government agencies that define rules and regulations for the company. An organisation needs to follow these rules. International Standardisations for Organisations (ISO) is the agency that sets rules for customers' information storage and use. An organisation may need a licence from these agencies to function.

The second group is normative consists media, non-government organisations, political parties and religious communities (van Woerkum and Aarts, 2008; Otubanjo and Amujo, 2012; Christensen, Morsing and Cheney, 2008). They promote the company's reputation and image to the funders and public (Arturo Lowensberg, 2010). To support business activities funders are needed (van Riel and Fombrun, 2007; van Riel, 1995). This requires companies to approach normative group to advocate their opinion about the products and services. Communication with this group can be associated with 'institutional theory' which suggests that organisations appear to influence peers through rules, requirements and social norms (Barringer and Harrison, 2000).

The third group is input that provides knowledge and other resources to help the business survive a fast-changing environment (Andersen, Kragh and Lettl, 2013). Communication with this group can be associated with 'resource dependence theory' which suggests that no organisation is self-sufficient (Barringer and Harrison, 2000). Experienced staff, financial partners, and skilled workers are required (van Woerkum and Aarts, 2008). These people influence businesses to exchange resources through communicating with one another (Arturo Lowensberg, 2010). The Resource Based View (RBV) theory is extended in Section 3.3.1 to understand the importance of knowledge and the people who generate it.

Services and products produced by an organisation are attractive to output groups such as customers and citizens (van Woerkum and Aarts, 2008). This is the fourth group and the one that buys these services. An output group is required to generate income.

The fifth group (Figure 2-6) is the group with comparable goals. This group may be able to provide domain specific knowledge, because it is comprised of similar nature of the organisations. This study concentrates on how an organisation explores knowledge from like mind people working in a similar domain. Therefore, communication is easier with a group with similar goals, such as those with whom is competing or collaborating. Joint effort towards a common goal is desirable. Communication with this group represents a 'stakeholder theory' which suggests that organisations form collaborations to reduce environmental uncertainties (Barringer and Harrison, 2000). To tackle identity thieves more efficiently, companies need to collaborate.

It is also important to consider how officials collaborate. Definitions discussed previously (Table 2-5) suggest multiple tactical and strategic media that facilitates organisational collaboration. Mechanism, media and channel often used interchangeably to refer to the mode of transmission of knowledge from a source to the destination. Shannon and Weaver (1949) consider media as a transmitted signal from one end to another. This suggest that media is "*conduits for knowledge*" (Jasimuddin, Connell and Klein, 2014, p. 196; Almeida, Hohberger and Parada, 2011, p. 394). Strategic media use an integrative approach to connect internal and external sources. Thus, it keeps track of difficult knowledge in a coherent way (Argenti, 2013). A centralised knowledge base discussed earlier (Section 2.3.3) is a good example. Members often perform many different functions at the same time by learning from various sources. An organisation requires coherent communication to keep track of the work done by thousands of employees situated at multiple locations. This thus help organisations to manage acquired knowledge from staffs. Tactical media such as in-house employee publications are shared internally amongst staffs to disseminate knowledge (Verčič, Verčič and Sriramesh, 2012, p. 225). Manager plays a mediator role between members and the management.

It is also important to select correct media that conveys message accurately (Shannon, 2001, p. 5). Dance (1970, p. 209) prescribed value from "*normative judgement*" is essential for clarity of the message. The media can generate noise. Therefore, requires appropriate mechanism for better understanding (Easterby-Smith, Lyles and Tsang, 2008). A media selection thus is an important in the knowledge sharing practice. An irrelevant media can bring ambiguity and create complexity in the shared content (Littlejohn and Foss, 2008, p. 190). Two commonly used communication mechanisms include formal and informal interaction, each with different pros and cons.

2.4.1 Formal Interaction

Formal interaction is a systematic approach to pre-identified activities (Ghaznavi *et al.*, 2011). This interaction is achieved through board meetings, dialogue with teams and presentations. In inter-organisational relationships, a formal knowledge flows in strategic alliances formation (Almeida, Hohberger and Parada, 2011). This thus requires a discrete mode of governance (van Wijk, van den Bosch and Volberda, 2011). Organisations work together to achieve one or more common goals (Arturo Lowensberg, 2010). Therefore, strategic alliances are formed between two or more companies with no joint ownership

(Lichtenthaler and Lichtenthaler, 2009). Strategic alliances are required for one of the following reasons such as to reduce cost, gain power and control, increase competitiveness, mitigate environmental uncertainties, gain knowledge and improve organisational learning (Arturo Lowensberg, 2010). Partners' discrete modes of governance are regulated by an official document (Hadjielias and Poutziouris, 2015, p. 869). The official contract is defined as:

> "A *specification of the actions that named parties are supposed to take at various times, as a function of the conditions that then obtain*" (Kaplow and Shavell, 2002, p. 29).

Action in the definition above refers to how a partner would behave in knowledge sharing process. They expect either equal knowledge from contributors or avoid information misuse from partners through the contract. The conditions referred to in this definition include the past actions of partners and future uncertainties. Trust may facilitate the elimination of risk of information misuse (Simpson, 2013a; 2013b) as extends the discussion in Section 3.4.2.

Mason and Leek (2008) discussed that networked relationships such as organised conferences and inter-firm reviews support knowledge articulation, because peers can meet face-to-face to share knowledge. Formal knowledge structures are found in the conferences whereby presenters and keynote speakers deliver lecture, leaflets and brochures (Almeida, Hohberger and Parada, 2011). Cifas (2014a) argues that industry specific newsletters help improve knowledge on current issues in the security profession. These meetings also contain some elements of informal discussion during tea breaks.

2.4.2 Informal Interaction

Most knowledge is shared through informal interaction and is facilitated by informal social ties (Styhre, 2011). Social norms such as moral character, ethical behaviour and past records of accomplishment govern informal gatherings (Hadjielias and Poutziouris, 2015). Interaction among peers is often achieved during meals, travels and coffee breaks (Ghaznavi *et al.,* 2013; Standage, 2013). Informal knowledge networks among organisations take a number of forms (van Wijk, van den Bosch and Volberda, 2011, p. 478-479). These include hiring experts from other organisations, social communities of practice, board-interlock, geographic and ethnic communities (Almeida, Hohberger and Parada, 2011).

Hiring experts from other organisations supports external knowledge sharing (Easterby-Smith, Lyles and Tsang, 2008). Almeida, Hohberger and Parada (2011) state that hiring across organisations lead both firms into informal inter-firm relationships, because security officers join the new company with past ties that provide firms a bi-directional knowledge flow. The people who move to another company maintain important ties that help them with specialised tasks.

Communities of practice also provide informal knowledge networks. A community of practice is comprised of a joint enterprise of mutual relationships to utilise shared repertoire of communal resources (Wenger, 1998). The concept was initially derived for beginners; it also pays attention on existing members of staffs (Almeida, Hohberger and Parada, 2011). Wenger (1998) suggests that members of a community are not only bound by what they do together but also by what they learn mutually. A community in the same region tends to provide a fluid mix of knowledge (Almeida, Hohberger and Parada, 2011, p. 387). This is consistent with informal social ties whereby structural and relational characteristics brings together knowledge holders (van Wijk, van den Bosch and Volberda, 2011).

2.5 Inter-Organisational Information Security Knowledge Sharing

Wang, Yuan and Archer (2006) showed that preventing identity theft requires all associated parties including an identity owner (registered member of the public), identity issuer (the government or private organisations issues an identity certificate), identity checker (custom or traffic police officer) and identity protector (the government legislation authorities or law enforcement agencies). They developed a framework of association among the stakeholders that show an information flow. This collaboration was established to share information among these stakeholders rather than knowledge. Information is merely being aware of something, whereas knowledge implies application of information to produce tangible result (Sanchez, 2005). In their framework, a victim of the identity theft reports a case of identity fraud to an issuing authority such as a bank. The bank then forwards the case to the law enforcement agency to take legal action. Thus, information flows from one stakeholder to another. This study does not take into account collaboration of the like mind officials from similar organisations. These officials can provide domain specific and improved learning experiences.

Majchrzak and Jarvenpaa (2004) considered ways to control information overflow from employees of collaborating organisations. Peers could leak company's private and confidential information during collaborations (Easterby-Smith, Lyles and Tsang, 2008). Securing important information is a key challenge in the knowledge management literature (Ahmad, Bosua and Scheepers, 2014). These authors did not consider identity theft or the security profession. They focused on how to avoid knowledge leakage in a broader collaborative environment. Few studies address information security knowledge sharing among security officials and are summarised as follows (Table 2-6).

Table 2-6: Information security knowledge sharing

Structure	***Mechanism***	***Relationship***	***Authors***
Web protégé	Online	Open source database (many government, military and commercial organisations)	Feledi, Fenz and Lechner, 2013; Feledi and Fenz, 2012; Mace, Parkin and van Moorsel, 2010; Stahl, Parkin and van Moorsel, 2011.
Complementary and standalone knowledge base	Offline and online mechanisms	Closed partnership (two to three commercial organisations)	Flores, Antonsen and Ekstedt, 2014; Liu, Ji and Mookerjee, 2011.
Forums - ISF, ITISAC, and Gartner Inc.	Offline and online mechanisms	Fraud forums – paid membership (many members from government and commercial organisations)	https://www.securityforum.org, http://www.it-isac.org, http://www.gartner.com/technology/home.jsp, and https://www.cifas.org.uk
LinkedIn groups - Information Security Group, Anti-Fraud experts		Virtual communities – closed membership (wide range of individuals from similar domain of work)	Tamjidyamcholo *et al.*, 2013; Tamjidyamcholo *et al.*, 2014 also see https://www.linkedin.com/groups/924757, and https://www.linkedin.com/groups/83088

Table 2–6 suggests four different types of relationships to gain knowledge from external organisations. The first is an open source relationship created by web protégé that assists various actors to add and edit their knowledge in a web-oriented community. In this relationship, officials may need no contractual governance. However, the second type of relationship such as partnership is based on an official agreement signed between two or more organisations. The partnership requires a closer collaboration and direct modes of communication. The contracts spell the explicit terms of knowledge exchange as

discussed earlier (Section 2.3.4). In the third and fourth relationships, security professionals may not have an official agreement or direct modes of communication with one another. However, they subscribe themselves with professional bodies by a membership scheme. Administration may have a pre-defined set of rules that guides members' behaviour, thus gaining members' trust (see Chapter 3, Section 3.4.2).

2.5.1 Open Source Database

Newcastle University's technical report series (Mace, Parkin and van Moorsel, 2010; Stahl, Parkin and van Moorsel, 2011) concentrated on Chief Information Security Officers (CISOs) from various organisations to capture knowledge. A community knowledge base was developed and shared centrally among the network of officials (Feledi, Fenz and Lechner, 2013). Stanford Centre for Biomedical Informatics (2016) defines a web protégé as:

> "*A Web Protégé is an ontology development environment for the web that makes it easy to create, upload, modify and share ontologies for collaborating viewing and editing".*

A web protégé is an open source software that provides tools to construct a web portal that captures domain specific knowledge in a community. This in turn help to avoid generating same security wheel implemented by the peers. Behavioural factors were measured to explore the reactions of the security officials. Even though the model was designed to help CISOs in policy-making decisions, it has several drawbacks. Firstly, there was little contribution from participants and incentives were needed to encourage members. Secondly, officials who were not adequately computer literate, found its use difficult. Thirdly, the model considered generic users from government, commercial and military organisations. The project maintenance and finance elements followed a public-private partnership model. This caused a lack of trust due to diversity of people involved in the project (Krogh, 2011, p. 418). To the overcome lack of motivation and distrust, Feledi and Fenz (2012), and Feledi, Fenz and Lechner (2013) added a feature which rewarded the user for his or her contribution. Lastly, the web protégé was designed on pre-defined themes such as vulnerabilities, threats, controls and ISO 27001. Consequently, inserting knowledge based on new innovative ideas is hurdle in the use of open source database.

2.5.2 Partnership

The partnership involves a signed agreement to secure complementary information system between two or three organisations (Liu, Ji and Mookerjee, 2011). Few studies have evaluated one-to-one relationships in the security profession (Flores, Antonsen and Ekstedt, 2014; Liu, Ji and Mookerjee, 2011). In the Liu, Ji and Mookerjee's (2011) study, a decision was made by two companies to share information security knowledge. Theoretically, they have calculated investment by the firms of equal sizes, so that there is approximate contribution of the knowledge sharing from each. A complementary information system was found to bring a natural incentive to share knowledge. However, to secure stand-alone information system, each organisation prefers to lock-in knowledge within its boundary. These findings are applicable only to companies of similar size.

Flores, Antonsen and Ekstedt (2014) investigated behavioural information security governance to explore how officials react to information security knowledge sharing activities. American and Swedish organisations were investigated. Results show that organisational risk appetite and performance limitations of the partner's knowledge hindered establishment of information security knowledge sharing. Performance limitation occurs due to insufficient knowledge from officials. The more risk tolerant companies found less incentive to learn from companies lacking in the ability to deal with identity thieves. These authors have further discovered that a centralised information security structure employs uniform firm level policies and a steering committee leading to sharing security knowledge. However, they failed to test company size and the industry in which firm operates. These characteristics may have helped to address impact of their decision to share knowledge. Even though official contracts were regulated, companies failed to help each other in to secure standalone information systems.

2.5.3 Forums

Many online forums and online virtual groups exist worldwide to secure organisations from cyber threats. Gartner, ISF, and IT-ISAC are the official bodies where security professionals can improve their technical skills by sharing learning experiences. Cifas is a dedicated forum devoted to online fraud in the UK. These forums are established to impart knowledge of information security officials to help detect and prevent identity theft. These forums promote best practice by reporting, sharing, gathering and analysing cross-sector information.

Information Technology – Information Sharing and Analysis Center (IT-ISAC)

IT-ISAC is a non-profit limited liability forum reputable to provide a network of relationships. It was established in 2000 however officially operated from 2001. The forum is running on membership fee in one of the categories such as Bronze ($3,000), Premium Silver ($8,000) and Foundation Gold ($25,000) (IT-ISAC, 2013a). It aimed to achieve situational awareness. Therefore, "*information sharing is a tool that enables situational awareness and informs actions*" (Algeier, 2015, p. 3). The forum serves IT companies from around the world (IT-ISAC, 2013b). Leading IT companies such as HP, Oracle and IBM are among its members. One of the online mechanism used by members to share identity frauds knowledge is "Operations Centre*"*. Operations centre is a real time point of contact whereby registered members gain immediate advice. Local members are connected through spatially clustered social networks (see http://www.internetsociety.org for the USA chapter and http://isoc-e.org for the UK chapter). The forum promotes trust through using non-disclosure agreement.

Information Security Forum (ISF)

The ISF is a not-for-profit information security forum established in 1989 in the UK. It aims to provide knowledge on cyber security, information security and risk management. It has a dedicated knowledge exchange section to provide officials' interaction. These include, ISF live, annual world congress, chapter meetings, solution development workshops, special interest groups. Similar to the Operations Centre from IT-ISAC, 'ISF Live' is a global online mechanism. It connects experts on various topics to provide specific help and provides offline mechanisms such as annual global congress and chapter meetings whereby security officials collaborate in-person to gain practical advice on key security challenges. Chapter meetings are organised across 25 countries several times a year to facilitate interaction among members located in the same region. Chapter meetings are confidential peer-to-peer networks to exchange ideas with ISF analysts and industry experts. ISF was also founded based on membership whereby members pay £27,000 annual fee for full membership.

2.5.4 Virtual Communities

A virtual community created for professionals with specialised knowledge to form an online community in an effort to exchange knowledge (Hsu *et al.*, 2007). These communities are based on members with common activities (Tamjidyamcholo *et al.*, 2013; 2014), which brings natural incentive to use shared knowledge for betterment of performance. LinkedIn groups such as the Information Security Virtual Community and the Anti-Fraud Experts are common examples of these communities (Table 2-6). These groups are subscription free with worldwide members. The group members can interact without meeting face-to-face (Hsu *et al.*, 2007). This provides an opportunity for worldwide collaboration without constrain of time and geographic barriers. A problem with this type of communication is that officials either have little or no active incentive to contribute (Tamjidyamcholo *et al.*, 2013; 2014). These groups are composed of people with different behaviours (Simpson, 2011). This means it requires a pre-defined set of rules to regulate members' interaction. These forums and virtual communities may be beneficial. However, for a large group of people it is hard to contribute knowledge and expensive to wait for someone to post something (Krogh, 2011, p. 418). Thus, resulting in no posts.

2.6 Development of the Research Questions

The forums and online communities discussed in the previous section are lacking an empirical investigation to explore views from real actors. Can knowledge shared through online communities and virtual groups reduce risk (Tamjidyamcholo *et al.*, 2014, p. 19)? There is urgent need for empirical studies to understand what is working in retail organisations and what does not seem to be providing benefit concerning knowledge to address and mitigate identity theft. Trust is also hard to find in online communities, because of large groups with members worldwide (Krogh, 2011, p. 418). For instance, the Anti-Fraud Experts group discussed comprised approximately 20,000 members (Table 2-6). Similarly, Gartner Inc. deals with 60,000 clients around the world. Many members consider shared information on online group either useless or fake. Consequently, some members either do not participate or have a small active role in sharing fraud prevention knowledge (Feledi, Fenz and Lechner, 2013; Tamjidyamcholo *et al.*, 2014). An incentive or reward system is needed to reinforce behavioural changes amongst security professionals (Feledi, Fenz and Lechner, 2013; Liu, Ji and Mookerjee, 2011). These challenges identified in the limited literature of information security knowledge sharing practice may help to address the following research questions: Firstly, the membership relationships in online fraud forum is lacking an empirical study to evaluate whether knowledge obtained from the forums is of value to address and mitigate identity frauds. This gap motivated the design of RQ1:

> *What is working for the retail sector organisations and what does not seem to be providing benefit with regard to knowledge sharing to address and mitigate identity theft?*

This question contains two components broken down as follows:

> RQ1 (a): What is working for retailers with regards to knowledge sharing to address and mitigate identity theft?
>
> RQ1 (b): What does not seem to be providing benefit with regards to knowledge sharing to address and mitigate identity theft?

Secondly, in the virtual relationships such as professional communities, Tamjidyamcholo *et al.* (2014, p. 31) noticed the need for a study that explores: *"Why some individual either do not take part or have less active participation in information security virtual community*". This study adapts this question into RQ3 as follows to explore behavioural aspect associated with individuals' use of online groups.

> *Why do some individual either not take part or have little active participation in information security knowledge sharing?*

This question also contains two components that measure security experts' reaction, such as no participation and less participation. RQ3 can be broken down as follows:

> RQ3 (a) Why do some security officials not take part in information security knowledge sharing?
>
> RQ3 (b) Why do some security officials have small active participation in information security knowledge sharing?

Thirdly, in the partnership relationship, members are reluctant to contribute their knowledge to help each other in securing stand-alone information systems (Flores, Antonsen and Ekstedt, 2014; Liu, Ji and Mookerjee, 2011). To explore this aspect, RQ2 was designed as:

> *To what extent are companies willing to share fraud prevention knowledge with each other and under which condition(s)?*

Similar to previous questions, this new question also has two aspects to explore from security officials designed as follows:

> RQ2 (a) To what extent are companies willing to share fraud prevention knowledge with each other?
>
> RQ2 (b) Under which condition(s) are companies willing to share fraud prevention knowledge with each other?

Many other questions in the domain of knowledge sharing in the information security remain unanswered. These studies neither focused on interactive dynamics between retail sector organisations nor the company size and characteristics to evaluate knowledge sharing practice (Flores, Antonsen and Ekstedt, 2014). These studies do not take into account the nature of knowledge being shared and the degree of tactitness, ambiguity, or complexity to help understand value in the knowledge (Easterby-Smith, Lyles and Tsang, 2008). Tamjidyamcholo *et al.* (2013) measured intention and attitudes of members of an information security virtual community with respect to trust, self-efficacy, reciprocity, and shared language. Their quantitative analysis does not consider information security professionals from retail organisations nor do they examine the identity theft prevention knowledge sharing. Their predictors are not all-inclusive as stated by them that:

> "*This study has tried to experimentally examine predictors of knowledge sharing intention and knowledge sharing attitude. But these predictors and constructs are not all-inclusive dimensions of knowledge sharing intention and attitude in information security virtual communities.*" (Tamjidyamcholo *et al.*, 2013, p. 231)

The need for a comprehensive study that explores individual and collective efforts towards external knowledge sharing practice is required in general (Krogh, 2011, p. 404) and in information security knowledge sharing practice in particular (Tamjidyamcholo *et al.*, 2013, p. 231). A framework of associated components seems useful efforts to evaluate and understand inter-organisational identity theft knowledge sharing practice in the retail sector. This aspect is considered in RQ4 as follows:

> *Which is the suitable knowledge sharing framework in security profession in retail that facilitates an understanding of an inter-organisational identity theft prevention knowledge sharing practice?*

2.7 Summary

Information security has hitherto considered a technical response as the main priority to address identity theft. Knowledge sharing as a strategic practice has attracted little attention. Several doubts exists whether information security knowledge shared on online forums (i.e. Gartner, Cifas, and ISF) is of value to prevent and mitigate identity theft. Researchers believe that technology supports the sharing of information rather than knowledge. An alternative view is that technology is an enabler of knowledge management activities. Concerning domain specific knowledge, this thesis argues that value gained from external knowledge cannot completely destroyed when shared using online forums. To investigate identified various assumptions require a framework of all-inclusive components. The next chapter evaluates three frameworks from recent literature to find suitability and applicability in the security profession in retail.

CHAPTER 3 CONCEPTUAL FRAMEWORK

3.1 Introduction

This chapter explores the theories relevant to retail organisations that facilitates knowledge sharing. This thus addresses RQ4 which seeks a suitable framework in online security profession in retail to facilitate inter-organisational identity theft prevention knowledge sharing. Three frameworks from recent literature on inter-organisational knowledge sharing have been compared to determine their suitability in security profession and application in online retail sector. The components of these frameworks are evaluated and summarised to propose an extension of the existing theory.

3.2 Framework

Why is it necessary to understand all-inclusive components in the inter-organisational knowledge sharing process and how does a conceptual framework help to obtain a better understating? Saunders, Thornhill and Lewis (2015, p. 545) emphases importance of the conceptual framework by using a jigsaw puzzle analogy as:

> "*Puzzle for which there is no picture are usually more challenging as we have no idea of the picture we are trying to create*".

A conceptual framework is a map the intellectual territory being investigated (Miles, Huberman and Saldana, 2014). Easterby-Smith, Lyles and Tsang (2008) suggested that understanding of a firm's inter-organisational knowledge sharing and associated components can enhance its capability. A theoretical framework represents certain phenomena relating one aspect to another (Sekaran and Bougie, 2013, p. 68). Knowledge sharing between organisations is a more complex process than knowledge sharing within an organisation (Yang and Maxwell, 2011; Bigdeli, Kamal and Cesare, 2013; Szulanski, 1996). This involves multifaceted nature of boundaries, processes and cultures, confidentiality and leakage concerns, legal aspects, communication skills and tools, instituted routines and social capital (Bigdeli, Kamal and Cesare, 2013; Styhre, 2011; Szulanski, 1996; Easterby-Smith, Lyles and Tsang, 2008). To understand how this phenomenon influences inter-organisational knowledge sharing practice in security profession, recent theories need to be evaluated. A conceptual framework seems useful effort to evaluate various themes involved in the inter-organisational knowledge sharing practice. Due to limited literature in information security knowledge sharing practice, selecting an appropriate framework to conduct this study is challenging. To assist the selection, three frameworks from recent literature are compared, contrasted and summarised in Table 3-1.

Table 3-1: Comparisons of theoretical frameworks

Framework (1)	***Framework (2)***	***Framework (3)***
Proposed factors of influencing electronic information sharing in local government authorities.	*The relationship of factors influencing inter-organisational information sharing.*	*Factors influencing inter-organisational knowledge transfer.*
To investigate facilitators and barriers of information sharing at local government authorities. The framework served as decision-making tool to consider whether sharing of information using electronic mechanism is useful.	To evaluate relationship among the factors associated with organisational information sharing activities.	Providing an understanding of inter-organisational knowledge transfer process and mapping current themes and future research areas.
Electronic information sharing and collaborations considering the public sector organisations.	Information sharing in the public sector organisations.	Knowledge transfer between the organisations to increase innovativeness, survival and competition.
Bigdeli, Kamal and Cesare, 2013	Yang and Maxwell, 2011	Easterby-Smith, Lyles and Tsang, 2008

3.2.1 Proposed Factors of Influencing Electronic Information Sharing

Bigdeli, Kamal and Cesare (2013) developed a framework of electronic information sharing to assess knowledge sharing practice in local government. Previous research extensively focused on central and federal government organisations and disregarded local bodies. Therefore, they found a need to consider local organisations to investigate an inter-organisational knowledge sharing process. They used theoretical lenses to evaluate a systematic literature review and devised a new framework of components illustrated in Figure 3-1.

The focus was on public sector local government organisations and the surrounding environment to assess impact of the decisions designed to share information using electronic systems. The authors viewed knowledge sharing as a central activity which surrounds external environment, inter-departmental environment, technological environment, characteristics of electronic information sharing, and capacity of organisation to absorb an external knowledge.

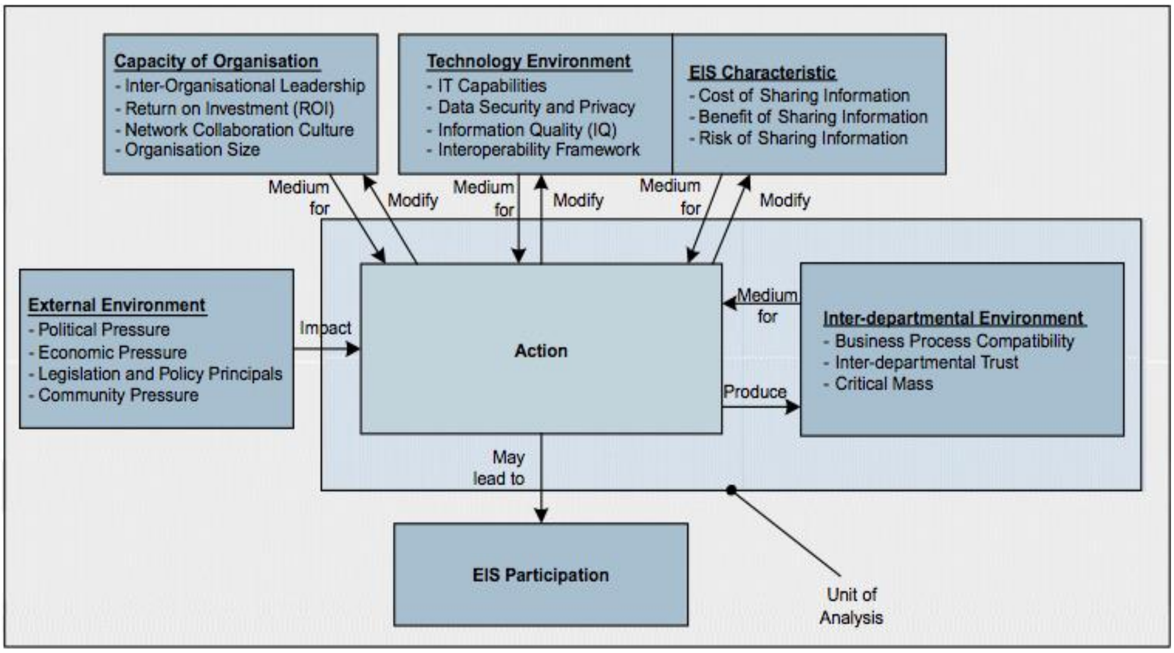

Capacity of Organisation
- Inter-Organisational Leadership
- Return on Investment (ROI)
- Network Collaboration Culture
- Organisation Size
Technology Environment
- IT Capabilities
- Data Security and Privacy
- Information Quality (IQ)
- Interoperability Framework
EIS Characteristic
- Cost of Sharing Information
- Benefit of Sharing Information
- Risk of Sharing Information
Medium for
Modify
Medium for
Modify
Medium for
Modify
External Environment
- Political Pressure
- Economic Pressure
- Legislation and Policy Principals
- Community Pressure
Impact
Action
Medium for
Produce
Inter-departmental Environment
- Business Process Compatibility
- Inter-departmental Trust
- Critical Mass
May lead to
EIS Participation
Unit of Analysis

Figure 3-1: Proposed factors influencing electronic information sharing in Local Government Authorities

Source: Bigdeli, Kamal and Cesare (2013)

These authors examined public sector organisations; several components in this framework are not relevant to assess retail businesses. The external environmental factors such as political pressure might not necessarily influence decisions made by the retailers to share knowledge. Retail is mainly a private sector profit-oriented. Retailers may face pressure from community for unnecessarily disclosing customers' private information to the partners. Components of the framework need to be tested and validated in practice.

3.2.2 Relationships of Factors Influencing Inter-Organisational Information Sharing

Yang and Maxwell (2011, p. 171) developed a framework of relationships and associated components that influence inter-organisational information sharing. This framework is useful in policy and legislation to help eliminate risk of leaking customers' private information in the collaboration. The components of this framework were designed based on public sector organisations. The framework was also based on insights obtained from literature. Therefore, similar to previous framework, its components need to be empirically tested and evaluated. The components of this framework are illustrated in the following diagram.

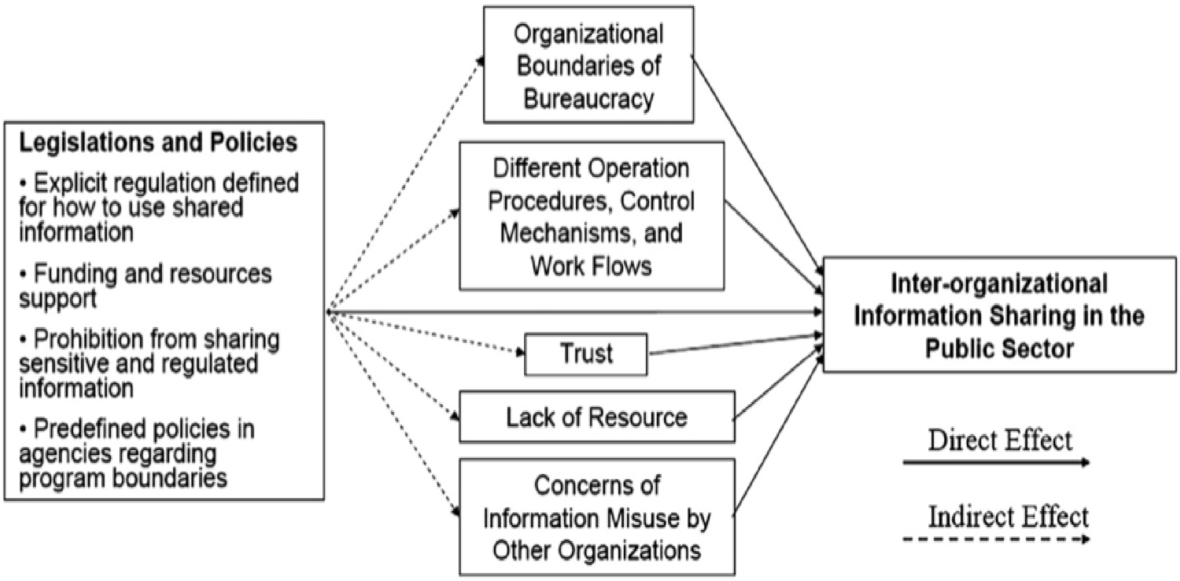

Legislations and Policies
• Explicit regulation defined for how to use shared information
• Funding and resources support
• Prohibition from sharing sensitive and regulated information
• Predefined policies in agencies regarding program boundaries
Organizational Boundaries of Bureaucracy
Different Operation Procedures, Control Mechanisms, and Work Flows
Trust
Lack of Resource
Concerns of Information Misuse by Other Organizations
Inter-organizational Information Sharing in the Public Sector
Direct Effect
Indirect Effect

Figure 3-2: Relationships of factors influencing inter-organisational information sharing

Source: Yang and Maxwell (2011)

In Figure 3-2, the factors such as political concern, external regulation and funding may not be key obstacles in retail business. Moreover, this framework focused extensively on explicit knowledge rather than tacit knowledge. The security professionals may contain practical wisdom synthesised from tacit and explicit (Section 2.3.1). Therefore, requires elements that also consider tacit knowledge sharing.

3.2.3 Factors Influencing Inter-Organisational Knowledge Transfer

Easterby-Smith, Lyles and Tsang (2008, p. 679) developed a framework of factors influencing inter-organisational knowledge transfer to help understand inter-organisational knowledge sharing practice. This framework considered future prospects on how companies share knowledge. They also focused on knowledge dissemination within a firm's boundaries. The reliability is devised based on six review papers published in the special issue on inter-organisational knowledge transfer in the Journal of Management Studies. These studies were conducted based on empirical examinations. The components of the framework have been evaluated through empirical investigation (Nylund and Raelin, 2015; Ho and Wang, 2015). The components of this framework are illustrated below.

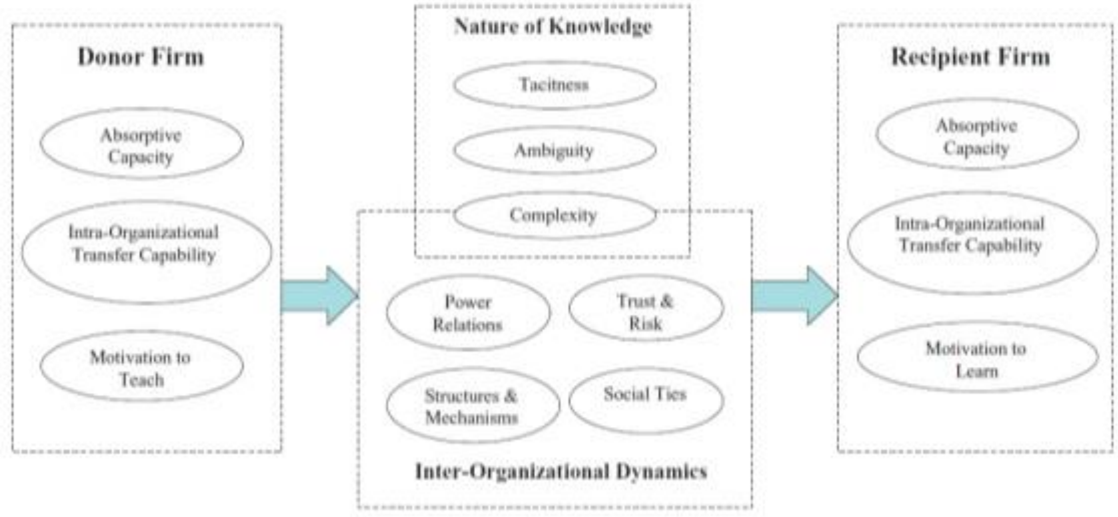


Figure 3-3: Factors influencing inter-organisational knowledge transfer

Source: Easterby-Smith, Lyles and Tsang (2008)

Several components in these three frameworks overlap. Firms' resources, capabilities, trust and risk are common in each framework. These are important factors to assess inter-organisational knowledge sharing. A distinct difference in these frameworks is in suitability and applicability in practice. In the first framework (Figure 3-1) authors considered factors influencing electronic information sharing and focused on the electronic environment. They have neglected the value of face-to-face interactions. The flow of knowledge is fluid when involves offline social communication (Nonaka, Von Krogh and Voelpel, 2006; Panahi, Watson and Partridge, 2013).

In the second framework (Figure 3-2), authors omitted value gained from tacit knowledge. Responding to identity theft may involve practical knowledge more than theoretical. Security officials' practical wisdom exists in their use of tacit knowledge (Tsoukas, 2011; Almeida, Hohberger and Parada, 2011). However, the frameworks in Figure 3-1 and Figure 3-2 did not address how tacit components embedded in the security officials' knowledge can be shared without ambiguity and complexity. However, some components from the first and second frameworks may be useful in the online retail sector. For instance, in the first framework the capacity of IT to share knowledge resources is useful. In the second framework concerns of losing autonomy of valuable knowledge going to competitors can be used. These factors may be useful to evaluate retailers' inter-organisational knowledge sharing practice.

The third framework (Figure 3-3) incorporates nature of knowledge being shared with characteristics that support external knowledge sharing. Inclusions of these components improve knowledge sharing practice. The third framework has been selected to explore knowledge sharing activities in the security profession. Components of this framework may be divided into three major categories. The first category concentrates on characteristics of donor and the recipient firm such as resources and capabilities to absorb new knowledge (knowledge absorptive capacity), structures and mechanisms to share new knowledge within the organisational boundaries (intra-organisational knowledge transfer capability), and motivation to teach and learn. The second category evaluates knowledge characteristics embedded in tacit and complex knowledge. The third category concentrates on inter-organisational dynamics that either facilitate or hurdle collaborations collaboration (power relations, trust and risk, social ties and structure and mechanisms).

3.3 Characteristics of Firms

Easterby-Smith, Lyles and Tsang (2008) discussed three capabilities to evaluate whether the company is equipped to gain and integrate external knowledge with its existing internal knowledge. Firstly, the firm's knowledge absorptive capacity underlies its staff abilities (experience, education, analytical skills). The security officials require relevant educational background to help prevent identity theft. Through frequent training programs, firms' knowledge sharing is supported (Elyas *et al.*, 2014). Secondly, how the company is providing the knowledge gained from external sources to its members in order to prevent identity theft. This is known as intra-organisational knowledge transfer capability which manifests itself in firm's internal communication practices and shared databases. Thirdly, the company requires tactics to recognise and reward security officials to engage in learning experiences. This is known as motivating technique. These three abilities are inter-related.

3.3.1 Knowledge Absorptive Capacity

Cohen and Levinthal (1990, p. 128) define knowledge absorptive capacity as "*The ability of a firm to recognise the value of new, external information, assimilate it, and apply it to commercial ends"*. The 'ability' referred is associated with security officials' knowledge base including skills, educational background and competencies (Junni and Sarala, 2013, p. 420). Minbaeva (2007) discovered that knowledge absorptive capacity is the dynamic capability within employees and is affected by specific skills possessed by individuals. This can be applicable to security teams working for different organisations. Organisations need to pay attention to its culture to enhance employees' knowledge base. Elyas *et al.* (2014) recently prescribed that people working in security profession require frequent training programs related to their roles and responsibilities. Otherwise, organisations may consider hiring qualified professionals (Harryson, Dudkowski and Stern, 2008). Harryson, Dudkowski and Stern (2008) also discovered characteristics of the staff that helped to explore and integrate new external knowledge in the organisational knowledge base. Following characteristics were found in members of the organisation who lead knowledge exploration and integration.

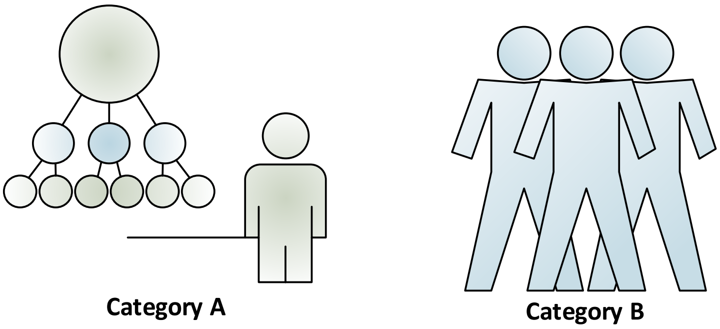


Figure 3-4: Characterises of staff that support knowledge exploration

Category A (Figure 3–4) is made of members that have broader vision, strong ties and power to bring the network structure. Harryson, Dudkowski and Stern (2008) call these people 'Spiderman', because they are situated at centre of the web of social ties. This category may be situated at the senior management position and is able to connect internal and external security official for fluid mix of knowledge that prevent identity theft.

Category B (Figure 3–4) is for staff with relevant and necessary work experience and insights. These people enjoy challenges, value innovative thinking, thrive in an independent environment and are part of something broader rather than doing their normal day-to-day activities. Information security analysts, identity theft specialists, IT-security professionals are common people in this category. These people have strong past ties and credibility with their parent organisations (Almeida, Hohberger and Parada, 2011; Harryson, Dudkowski and Stern, 2008).

In strategic management, an RBV theory is related to knowledge and the people who generate it. RBV theory explains how businesses exploit available resources such as processes, people, capital and knowledge to maximise efficiencies. Barney (2000; 1991) defines RBV as firm's valuable non-substitutable and inimitable resource that leads to competitive advantages. The theory was initially designed to consider an internal resource. The theory now reflects on external resources such as knowledge (Sammarra and Biggiero, 2008, p. 802). Shaw, Park and Kim (2013) measured an RBV of a firm from human capital perspective by arguing that:

> *"When human capital accumulations are high, a company is likely to profit from firm-specific skills, knowledge, and abilities to sustain competitive advantage."* (Shaw, Park and Kim, 2013, p. 574)

They thus suggest that organisation can lose important knowledge when they are unable to retain their security officials. Exchanging skilled information security members with other retailers thus may be beneficial in informal ties (Almeida, Hohberger and Parada, 2011, p. 387). However, there is also a loss of competitive knowledge acquired during employment.

Another mainstream that enhances knowledge absorptive capacity is holding prior relevant knowledge (Cohen and Levinthal, 1990; Jansen, Van Den Bosch and Volberda, 2005). In other words, security officials working in the same field can acquire external knowledge quickly. They would be able to understand easily what their peers are doing. Thus, members' acumen, creativity, memory and volition have a positive impact in absorption of new knowledge (Ringberg and Reihlen, 2008, p. 912). A firm also absorbs new knowledge quickly if it finds something valuable from its donors (Pérez-Nordtvedt *et al.*, 2008). The question is how knowledge coming from other security officials is valued and used to prevent identity theft. Pérez-Nordtvedt *et al*., (2008, p. 714) used constructs such as knowledge rareness, non-substitutability and inimitability to evaluate value of the knowledge gained. These are the characteristics surrounded in tacit knowledge. Measuring value associated with tacit knowledge is challenging (Easterby-Smith, Lyles and Tsang, 2008, p. 681). Thus, this thesis chose to explore whether online retailers apply external knowledge to prevent identity theft or integrate with existing knowledge base of the firm rather than knowledge rareness, non-substitutability and inimitability.

3.3.2 Intra-Organisational Knowledge Transfer Capability

Easterby-Smith, Lyles and Tsang (2008, p. 687) suggest that there is no benefit to explore external knowledge if it is not used by members. Thus, both intra-organisational and inter-organisational communication are equally important in the knowledge management capacity. Internal communication practice helps knowledge exploitation and use. Thus, may lead security officials to apply new knowledge effectively. Easterby-Smith, Lyles and Tsang (2008, p. 679) believed that a firm which is good in absorbing new external knowledge, must also be well equipped to diffuse knowledge within its boundaries. This is also consistent with Nonaka *et al.* (2014, p. 139) that:

> "*Separation between exploration and exploitation is merely artificial;*
> *and that does not exist in actual practice"*.

Intra transfer capability refers to equipment and ability of internal staff to communicate with each other and share their learning experiences (Easterby-Smith, Lyles and Tsang, 2008). Cornelissen (2014) provides examples of internal communication medium by use of newsletters, promotion packages, corporate design and code of conduct. The role of centrally shared repositories and knowledge base is discussed (Section 2.3.3). An organisational memory assists knowledge exploitation where a new knowledge is integrated into existing knowledge base and can be retrieved by the security officials to put into practice (Klein, Connell and Jasimuddin, 2007).

Chapter 2 (Section 2.4) mentioned that employee-oriented publications are used in disseminating knowledge among staffs. Internal publications or magazines lead to better internal knowledge sharing regardless of whether it is hardbound printed copy or an online attachment. In addition to television as traditional news outlets, Argenti (2013) has discovered that people also learn when they engage in visual mediums such YouTube videos and social media blogs. Company owned intranet also facilitates internal collaboration whereby management can easily approach employees, quickly and widely (Argenti, 2013, p. 183).

Social media applications are useful for managers to disseminate important knowledge in the organisation (Fieseler and Ranzini, 2015; DiStaso, McCorkindale and Wright, 2011). Wright and Hinson's (2010) longitudinal study investigated social media application such as Facebook, LinkedIn, Twitter, blogs and YouTube videos. They have found that Facebook and LinkedIn groups are forefront in the workplace to disseminate knowledge.

Approximately 77% of staff used social media applications (Wright and Hinson, 2010). Email, blogs and social networking sites enable officials to become communication manager (Cornelissen, 2014, p. 164). Fieseler and Ranzini (2015) and Almeida, Hohberger and Parada (2011) considered these applications from a personnel image perspective. Profiles designed on LinkedIn are helpful to generate professional impression. Thus, it leads to online reputation and access to external knowledge.

However, behavioural response to these applications could be threatening, because employees fail to control how other people will respond to the shared content (DiStaso, McCorkindale and Wright, 2011, p. 326). The use of social media applications at workplace can bring a number of challenges including criticism from management. Until now, few studies have considered severe impact of social media groups in information security knowledge sharing practice (Feledi, Fenz and Lechner, 2013; Tamjidyamcholo *et al.*, 2014). Therefore, behavioural responses need to be explored further with respect to how identity theft specialists use social media to enhance their learning abilities (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Feledi, Fenz and Lechner, 2013), and whether do they need permission from management to share their knowledge through social media groups.

3.3.3 Motivation to Teach and Learn

IT security professionals in many organisations are fighting alone to tackle identity theft (de Crespigny, 2012). They are assumed to have a natural incentive and intrensic motivation to learn from each other’s experiences (Liu, Ji and Mookerjee, 2011). However, official are sometime unwillingly contribute their knowledge in the knowledge sharing practice. Some members also find problem in collaborating with others (Wei, 2010). The challenge involved is how to apply natural incentive if knowledge sharing is an invisible activity that cannot be easily monitored (Easterby-Smith, Lyles and Tsang, 2008). Also incentives and reward systems needed to reinforce behavioural changes amongst security professionals (Feledi, Fenz and Lechner, 2013; Liu, Ji and Mookerjee, 2011). Van Wijk, Jansen and Lyles (2008), Vaara *et al.*, (2012), and Wei (2010) found that employees negatively react to knowledge sharing process if their knowledge is insufficient.

A relational view that supports manager to achieve employee motivation is their frequent communication (Verčič, Verčič and Sriramesh, 2012). Lopez and Esteves (2013) have investigated underlying characteristics of inter-wined network in knowledge acquisition process. They have explored internal and external networks and discovered that top managers are the champions to enhance knowledge sharing practice. Similarly, Easterby-Smith, Thorpe and Jackson (2012, p. 3) have evaluated human relational theory and found that a managers require an understanding of staff's personal values. The knowledge of employees' values helps managers to explore how their teams can be more effective. Thus, may help to overcome problems with knowledge holders' lack of motivation (Feledi, Fenz and Lechner, 2013; Fenz, Parkin and van Moorsel, 2011).

3.4 Inter-organisational Dynamics

Interactive dynamics such as power relations, trust and risk, structure and mechanisms and social ties between firms need to be understood to lead organisations in the inter-organisational knowledge sharing process (Easterby-Smith, Lyles and Tsang, 2008). These dynamics are the capabilities of a firm that adapts internal and external resource configurations and processes by considering shifting needs and market condition in pursuit of competitive advantages (Verona and Zollo, 2011). Tece, Pisano and Shuen (1997) confirm that dynamic abilities help organisations to integrate, build and reconfigure internal and external competencies.

3.4.1 Power Relations

Power is "*a force that influences outcomes*" (Hardy, 1994, p. 220). A leading organisation benefits from dependency relationships to get work done since they depend on shared knowledge (Lotia, 2004). Organisations often find themselves in learning races to gain competitive advantage (Barney and Hesterly, 2015, p. 74). However, a 'win-win' situation is challenged by the shared asymmetrical power (Eaterby-Smith, Lyles and Tsang, 2008) and pressure of serving personal interest. A quick learning sub-ordinate may become a competitor and may either eliminate cooperation or provide knowledge of lower quality (Easterby-Smith, Lyles and Tsang, 2008). Consequently, competent organisations fear to lose knowledge of higher quality to partners (Yang and Maxwell, 2011). Therefore, mutual trust needs to be reinforced to tackle knowledge asymmetry (Dale Stoel and Muhanna, 2012), otherwise organisations may lock-in practices of identity theft prevention within their boundaries (Barney and Hesterly, 2015; Gaur *et al.*, 2011).

3.4.2 Trust and Risk

Trust is perception of partner's behaviour and expectations (Simpson, 2013a; Gaur *et al.*, 2011). Trust is also a question whether one partner is willing to accept vulnerability from other's actions (Becerra, Lunnan and Huemer, 2008). Trust is an invisible assumption (Simpson, 2012, p. 550); it depends on relationships of knowledge provider and the seeker (Simpson, 2013a; Gaur *et al.*, 2011; Becerra, Lunnan and Huemer, 2008). Trust between firms is the relationship among the people and is built upon exchange of characteristics (Gaur *et al.*, 2011, 1754). It is not a 'free hanging' element, nor does refer to the nature of a single phenomenon (Simpson, 2013a; 2013b). It has no deterministic rule to use. It is sustained through relational setting (Six and Sorge, 2008) whereby quality of a person of being trusted requires transparency, reliability, consistency and predictability (Becerra, Lunnan and Huemer, 2008, p. 692). These elements are sustained through someone's past actions (Simpson, 2011) such as ethical behaviour, non-egocentric nature, professional fulfilment and emotional evaluation, (Becerra, Lunnan and Huemer, 2008; Simpson, 2013b).

Trust literature in inter-organisational relationships covers two aspects. The first, it involves peers' trust to share important knowledge with each other (Becerra, Lunnan and Huemer, 2008). The second is whether shared knowledge is trustworthy and valuable (Tamjidyamcholo *et al.*, 2013). The first question involves knowledge holders' characteristics such as integrity, moral responsibility and relational bonding (Simpson, 2013a; Becerra, Lunnan and Huemer, 2008; McMyler, 2011; Faulkner, 2014). The second question however concentrates on knowledge characteristics than persons' such as knowledge usefulness, value, rarity and non-substitutability (Tamjidyamcholo *et al.*, 2013; Easterby-Smith, Lyles and Tsang, 2008; Pérez-Nordtvedt *et al.*, 2008).

The dimensions of trust and distrust exist simultaneously due to possibility of risk and relational dependency (Easterby-Smith, Lyles and Tsang, 2008; Becerra, Lunnan and Huemer, 2008; Welch, 2006). It is hard to achieve trust in the security profession (Tamjidyamcholo *et al.*, 2013). It is even more complex in networked relationships (Simpson, 2011, p. 29), because *"some people use the anonymity of the web to behave very badly indeed*". Confidentiality and leakage also compromise cooperation among the organisations (Easterby-Smith, Lyles and Tsang, 2008; Ahmad, Bosua and Scheepers, 2014).

Easterby-Smith, Lyles and Tsang (2008, p. 680) suggest that, "*Trust facilitates knowledge transfer by creating a sense of security that the knowledge in question will not be exploited beyond what is initially intended*". These characters help senders of knowledge to justify what they know. These characters also help receivers of the knowledge to ensure that it will not be used inappropriately. A competing firm often finds easy to influence others, because others depend on its knowledge (Gaur *et al.*, 2011). In either situations, it requires contractual governance to demonstrate trust in the inter-organisational bonding (Gaur *et al.*, 2011, p. 1775).

Trust in offline environment is easy to achieve by observing partners. However, trust is hard to achieve in virtual relationships such as LinkedIn groups (Tamjidyamcholo *et al.*, 2014), as knowledge holders are unable to provide opinion about one another. Discussing eBay's reputation, Simpson (2011) argues that customers' track record of past trustworthiness provides evidence to future trustworthiness. This addresses B2C relationship which however is different than B2B relationships. In B2B relationships there are fears associated with losing competitive knowledge to the partner (Yang and Maxwell, 2011; Easterby-Smith, Lyles and Tsang, 2008). Virtual groups are able to gain reputation they handle their informants' intention. This is echoed as follows:

> "*So long as this group or network also expects trustworthiness of each member, and is prepared to sanction the untrustworthy by expulsion or other punishment, so the trustee's interest in maintaining membership in good standing in groups provides incentive for trustworthiness*" (Simpson, 2013b, p. 546)

Information security groups created on LinkedIn lack members' participation (Tamjidyamcholo *et al.*, 2013; Tamjidyamcholo *et al.*, 2014). An unattractive nature of the group is a possible reason (Simpson, 2013b). A member in the group finds no value from on-going membership. A reputed network is able to achieve trust easily, because "*Trusting individual is often rational in virtue of trustworthiness of the groups which they are member of*" (Simpson, 2013b, p. 549).

It is also wise to understand risk associated with membership to gain trust. Becerra, Lunnan and Huemer (2008) have found that companies fear when they share explicit knowledge. Sharing a document is riskier, because it can be reproduced. A receiver can replicate a copy of the document to use against the senders. Similarly, a receiver is concerned with the waste of time if knowledge they receive is of lower quality or inaccuracy. To overcome issues with leakage the role of confidentiality agreements and code of conducts are essential (Ahmad, Bosua and Scheepers, 2014; Luoma, Paasi and Valkokari, 2010). However, trust and risks have yet to be explored in the online retail to evaluate how knowledge of identity theft practices is shared among security officials.

3.4.3 Structures and Mechanisms

Knowledge structure in an organisation is different from the interactive dynamic structures between the organisations. The former focuses on content such as organisation's cognitive templates, storage and transactive memory (Ahuja and Novelli, 2011). The latter however focuses on the context in which knowledge sharing takes place (Easterby-Smith, Lyles and Tsang, 2008). This section focuses on the second.

Structure is known as a context developed within a time and space that facilitates identity theft prevention specialists to interact (Nonaka *et al.*, 2014). Easterby-Smith, Lyles and Tsang (2008) provide its two examples as strategic alliances whereby significant amount knowledge is shared among the organisations and the networks where security officials are members. Relationships between organisations are actually the structure among identity theft specialists in a dialectic process. Within a particular context an individual endowed with the practical power to transform the environment (Nonaka *et al.*, 2014). Therefore, requires a particular mechanism to share knowledge (Easterby-Smith, Lyles and Tsang, 2008, p. 680). Easterby-Smith, Lyles and Tsang (2008) suggest few common examples of knowledge sharing mechanism as, training members of the recipient firm, transferring experienced personnel, planned socialising activity and offering blueprint, hardware and document.

Specialised knowledge to resolve complicated identity theft cases at work can easily be shared using offline interaction (Ghaznavi *et al.*, 2011), because it is not only mixing people but also the solutions created (Nonaka, 1994; Nonaka and Takeuchi, 1995; Marshal and Novic, 1995). Mixing security officials from across different retailer can be costly and time consuming. Digital mechanism can overcome this hurdle as explained. Kaufman (1966) was the first to initiate the idea of digital communication systems. He advised managers in business organisations to think beyond their organisational boundaries and developed a data processing system by connecting various actors together. These structures are widely known as inter-organisational systems referring to an automated information system shared by two or more companies to contribute productivity, flexibility and competitiveness (Cash and Konsynski, 1985). Kumar and Van Dissel (1996) and Hughes, Golden and Powell (2003) described an inter-organisational system as a means of developing strategic alliances. These systems provide avenues for collaborative knowledge where shared repositories of knowledge are centrally shared with the members (Chi and Holsapple, 2005). This enhances learning skills through multiple relationships via electronic communication and integration of real-time interrelated business processes (Strader, Lin and Shaw, 1998).

An inter-organisational system offers quick communication. It extends reach, increases quality, decreases the cost and enables tight integration among firms (Walsham, 2001). Inter-organisational systems are collaborative models to improve bonding decrease behavioural uncertainties and provide collaborative opportunities (Chi and Holsapple, 2005). Including centralised automated systems, an inter-organisational knowledge sharing also uses many other facets of technology such as instant messaging, group discussion boards and video chat (Hartley, 2013). These also utilise online virtual communities on LinkedIn (Tamjidyamcholo *et al.*, 2013; Pinjani and Palvia, 2013). Online forums, blogs and social networks are used in the security profession (Tamjidyamcholo *et al.*, 2013; 2014) and facilitate knowledge holders around the globe and dictates the context mentioned in the Cyber Ba (Nonaka, Von Krogh and Voelpel, 2006)

Many organisations have implemented inter-organisational systems (Rajaguru and Matanda, 2012). Common examples are university and business research collaboration (Kyoung-Joo, 2011), supply chain management collaboration (Knoppen, Christiaanse and Huysman, 2010; Shih *et al.*, 2012; Du *et al.*, 2012) and manufacturing (Fang *et al.*, 2012). Online retail lacks this aspect from research to evaluate the kinds of mechanism used by the security officials in the online retail.

3.4.4 Social Ties

Since knowledge exploration is associated with tacit knowledge (Nonaka *et al.*, 2014), therefore requires informal social ties (Easterby-Smith, Lyles and Tsang, 2008). These informal social ties utilise structural and relational characteristics (van Wijk, van den Bosch and Volberda, 2011).

3.5 Nature of Knowledge

There is on-going debate on whether formal and informal interaction supports sharing of multiple types of knowledge (Sammarra and Biggiero, 2008). The role of ICT is discussed to explore complex elements embedded in the tacit knowledge to overcome time and geographic constraint among the peers. The notion of degree of tacitness is important when examining the type of knowledge shared in a specific context (see Section 2.3.1). This will lead whether tacit knowledge can be understood when shared using computer mediated mechanisms (Easterby-Smith, Lyles and Tsang, 2008; Junni and Sarala, 2013) or requires closer face-to-face collaboration for further clarifications. Tacit knowledge is deeply structured in skilful actions, as a result official often find it hard put into words that "*how they do what they do*" (Tsoukas, 2011, p. 455). How do researchers claim that tacit knowledge shared through social media can be articulated (Panahi, Watson and Partridge, 2015)?

Nonaka *et al.* (2014) notice that soft experiences such as IT skills commonly found in tacit knowledge. The knowledge that security officials hold may be comprised of synthesis of tacit and explicit knowledge (Figure 2-3). Tacit knowledge needs both sender and the receiver in person for its articulation. Tacit also needs interactive environment, sense of collegiality, shared language and intense communication (Nakano, Muniz and Batista, 2013). These constructs are commonly found in face-to-face interactions (Nonaka and Takeuchi, 1995). The ability of ICT applications that support tacit knowledge sharing needs to be explored without adding complexity and ambiguity (Tsoukas, 2011; Ribeiro and Collins, 2007; Styhre, 2004). Panahi, Watson and Partridge (2015, p. 8) have found that sharing of tacit requires documentation. This implicitly suggests that it needs to be converted into explicit (see Section 2.3.2). This supports

Nonaka’s conversion model (Figure 2–4) and eventually the spiralling model (Figure 2–3). Panahi, Watson, and Partridge’s (2015) study focused on a single profession such as physicians. They have discovered that to keep updated information physicians subscribe medical blogs which post improved insights. Physicians who use knowledge shared at social media such twitter feed and RSS feed, are active in their role than others who use conventional methods.

Social websites do not bring knowledge holders’ in person to clarify what they do, because shared tacit knowledge converted into explicit feeds articulation among the professionals. This can be evaluated from Tsoukas (2011, p. 453) “*familiar patterns*” which promote awareness of how their tasks are accomplished. Panahi, Watson, and Partridge (2013; 2015) conducted study in the domain specific whereby peers make use of familiar patterns in the work. Familiar pattern of knowledge in the security profession requires an investigation to explore whether security officials are able to articulate what their peers do. Online retail a study that explore these elements in the security profession. This aspect requires understanding whether identity theft specialists are able to understand knowledge shared by their peers. This study can apply this theory, as only security profession is involved than other group of people.

3.6 Summary

This chapter focused on RQ4 to evaluate frameworks by identifying a model useful in the security profession in retail sector. Three frameworks in inter-organisational knowledge sharing practice were selected and components of the framework discussed to identity current themes. In particular, benefits from the knowledge sharing initiatives are addressed. Knowledge sharing is of significance in the security profession. However, the frameworks evaluated raised many concerns including whether domain specific knowledge holders are able to prevent identity theft. These aspects consider security officials’ nature of knowledge to evaluate whether retailers are able to understand practices used by other peers. This chapter has also pointed out whether online fraud forums are able to provide invaluable knowledge that prevents identity theft. Is there any benefit from knowledge gained from non-domain retailers that prevents identity theft? The frameworks discussed are useful and may be extended to evaluate these questions. To explore these issues, this thesis proposes an extension to the framework illustrated in Figure 3-3 by synthesising these components into a new framework. The frameworks discussed in this chapter are generic in nature and broadly cover information than knowledge sharing. These frameworks can be applied to retail sector for the first time to evaluate information security knowledge sharing practice. The components discussed need to be empirically examined and synthesised in the workplace. The next chapter details out how this study is designed to investigate security professionals and the methods employed to collect and analyse data.

CHAPTER 4 RESEARCH METHODOLOGY

4.1 Introduction

This study was conducted by collecting and analysing empirical data based on an understanding of the devised framework (Figure 3-3) to interpret the data. This chapter discusses how this study was conducted, and what methods were followed which in turn reflect on methodological literature. The chapter is set according to the research onion model (Saunders, Thornhill and Lewis, 2015, p. 124), and unfolds the research process by peeling away successive layers (Figure 4-1).

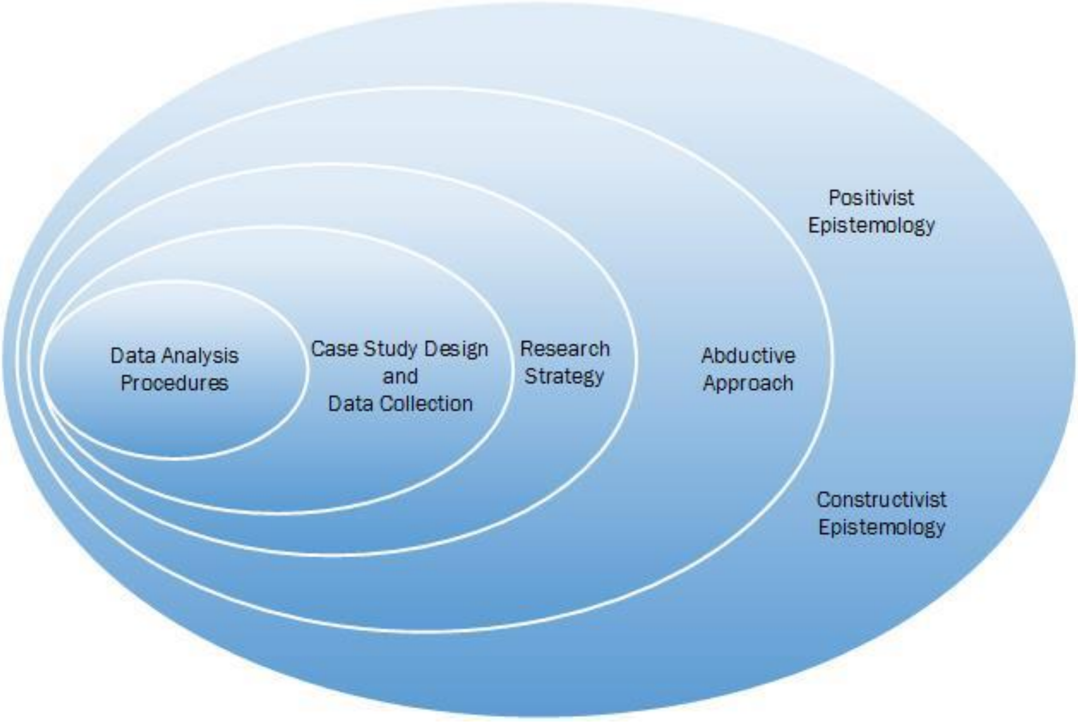


Figure 4-1: The research 'onion'

Adapted from Sounders, Lewis and Thornhill (2015).

The chapter begins by discussing the philosophical underpinning of the current research by discussing positivist and constructivist approaches applied. This represents the first layer in the research onion. An abduction approach is adapted in this thesis and explained as the second layer. This study adapts a mono-method qualitative methodology by employing multiple case studies as the research strategy. This represents the third layer. The design of the case study is also explained followed by data collection methods. This fourth layer considers design of an interview protocol and research ethics. Introduction of the research site is also given. The innermost layer explained data analysis procedures. Finally, the chapter is then summarised by discussing field visits.

4.2 Research Philosophy

The philosophical underpinning of the thesis concentrates on both what is researched and the researcher's position. For instance, "*whose story is it – the researcher or the researched"* (Pillow, 2003, p. 176)? This understanding brings a number of benefits, and Pillow based the question on Hans-Georg Gadamer (1960). Gadamer is a German philosopher, known for his work on hermeneutics 'Truth and Methods'. According to Gadamer, a researcher who belongs to a similar tradition may constitute more evaluative knowledge. This thesis, however, in contrast to Gadamer's view, suggests that an inquirer from a different tradition is able to notice differences that an investigator from a similar tradition might have taken for granted. A researcher with a similar tradition would intrinsically understand more of the situation and would question fewer things.

An understanding which shows the researcher's position in the study, contributes to an exploration of the intellectual investigative rationale and nature of valid and proper method (Hughes and Sharrock, 1997). The collective beliefs that guide a researcher to evaluate valid output are widely known as research philosophy, paradigm, pattern, model or frameworks (Easterby-Smith, Thorpe and Jackson, 2012; Crotty, 1998; Kuhn, 1996; Silverman, 2013). An understanding of the philosophical underpinning of the thesis improves the quality and contributes to the creativity (Easterby-Smith, Thorpe and Jackson, 2012). It helps in the extension of knowledge based on precision and reality (Kuhn, 1996). This understanding also helps to evaluate which research design is suitable to understand the nature of the topic, and enables a satisfactory outcome from the research process (Easterby-Smith, Thorpe and Jackson, 2012).

To explain the philosophical underpinning of the study and nature of the valid method, this thesis refers to the data highlighted in Table 4-1 (Column 3). The data highlighted suggests that this study is relativist that incorporates a constructivist approach. This study starts with the design of the key research questions (Chapter 1, Section 1.3 and Chapter 2, Section 2.6) to seek appropriate answers from information security officials working in online retail. This study draws from four cases (ShoppingCo, PaymentCo, TeleCo and

NetworkingCo). These four organisations help to understand other similar organisations such as how they prevent identity theft through sharing learning experiences. Convergence of these four cases may help a better understanding of similar phenomena. This study also uses qualitative data consisting of words and numbers for triangulation and comparison of different cases. In short Table 4-1 (Column 3) reflects that this study requires grounded theory. However, unlike grounded theory that focuses on induced data only (Saunders, Thornhill and Lewis, 2015), this thesis in addition concentrated on phenomena discussed in the conceptual models (Chapter 3).

Table 4-1: Methodological implications of different epistemologies

Ontologies	**Realism (1)**	**Internal Realism (2)**	**Relativism (3)**	**Nominalism (4)**
Epistemology Methodology	Strong Positivism	Positivism	Constructionism	Strong Constructionism
Aims	Discovery	Exposure	Convergence	Inversion
Starting point	Hypothesis	Proposition	Questions	Critique
Design	Experiment	Large surveys, multiple cases	Cases and surveys	Engagement and reflexivity
Data types	Numbers and facts	Numbers and words	Words and number	Discourse and experiences
Analysis/ interpretation	Verification/ falsification	Correlation and regression	Triangulation and comparison	Sense making and understating
Outcomes	Confirmation of theories	Theory testing and generation	Theory generation	New insights and action

Adapted from Easterby-Smith, Thorpe and Jackson (2012)

4.2.1 Positivism

Positivism is a belief that "*the researcher should be objective, maintaining complete independence from the object of study"* (Easterby-Smith, Thorpe and Jackson, 2012, p. 49). These authors however contradicted this positivist belief. They consider that measured knowledge properties require subjectively inferences such as sensations, reflection or intuition. These authors do not agree with positivists when an inquiry involves social realities. They also assert that positivist thinking can only be applicable in a context where a researcher investigates a phenomenon associated with the field of natural sciences. An experiment or a practice can be useful in reconstructing knowledge based on previous understanding in the natural sciences (Kuhn, 1962). However, a researcher’s independence is hard to sustain in the social sciences. Ringberg and Reihlen (2008) support an argument that knowledge of an objective entity cannot be comprehended without engaging the cognitive mind. Positivism concentrates on the richness of communication channels and absorption capability rather than ability of mind and interpretability. This thesis represents an understanding which is socially constructed with investigators, and synthesising with previous theories. These activities requires mind, intuition and sensation, rather than relying on richness of media. As a result, positivist approach is considered as eliminated in this study.

4.2.2 Constructivism

Constructivists challenge the assumption that meaning can be embedded in texts apart from the perceiver (Ringberg and Reihlen, 2008, p. 915). They believe that, the truth is underlying in one’s perspective, and each individual constructs meaning differently based on his or her intuition (Crotty, 1998). Reihlen and Ringberg (2006) have examined the role of computer-mediated knowledge management systems in consultancy firms. They have found that people perceive knowledge artefacts differently depending on their understanding, interpretation and comprehension abilities. Everyone is different and knowledge comprehension of the world depends on individuals’ cognitivists, constructivism, and experientialism. Social and contextual models also affect this comprehension.

Easterby-Smith, Thorpe and Jackson (2012, p. 23) argue that, “*Reality is determined by the people rather than objective and external factors*”. A knowing mind requires interaction with the world to understand reality (Nonaka, 1994; Wilson, 2002). The nature of this topic is explorative to understand how individuals in the security profession interact with external organisations to make sense of how other people produce solutions to prevent identity frauds. Therefore, constructivism is utilised whereby an understanding of the phenomena is achieved by continuous dialogue between previous theories (Chapter 1 to Chapter 3) and continuously interacting with social actors.

Constructivism is related to relativist and nominalist ontologies where there is no clear reality (Easterby-Smith, Thorpe and Jackson, 2012). Therefore illuminating truths via establishing claim supports the reality. There is a wide range of methodologies which can fit in the constructivism paradigm (Table 4-1), and the most notable is the case study as addressed in.

The starting point of constructivism paradigm is always the main research question(s) or the critique (Easterby-Smith, Thorpe and Jackson, 2012). This is similar in the context of the present study. This study starts by inquiring into the key research questions based on the gap found in previous literature. Methodological implications are associated with different epistemologies. Table 4-1 shows that the cases and surveys have a prominent link to relativism and constructivism. However, the ability of case studies is to investigate the context (Yin, 2009). Therefore, a case study methodology is selected to explore the research topic.

4.3 Research Approach

Abduction approach is used in this thesis. An abduction is one of the three form of the logical arguments used in the social science based inquiry. Social scientists use either deductive approach or inductive approach to inquire into a phenomenon, or they combine advantaged from the two called an abduction. Social scientists either test the theory or build a new one (Bryman and Bell, 2015, p. 20). Testing theory is associated with deductive reasoning, whereas theory generation is associated with inductive reasoning. In a deductive approach, theory guides a researcher, whereas in an inductive approach the theory is the outcome of the research process. The problem with deduction is that it relies on strict logic to support or reject a hypothesis. This approach eliminates the value of welcomed new surprises. However, an induction faces a criticism, whether the amount of empirical data is sufficient to develop a new theory. Abduction eliminates disadvantages of both approaches, as it considers help from previous theories, and helps to generate the new theory. An abductive approach allows thinking rationally whereby an understanding is developed through a continuous dialogue between the data and a pre-understanding. A pre-understanding supports performing the empirical scrutiny effectively (Yin, 2009). The existing theoretical framework helps with data analysis (Bryman and Bell, 2015). Figure 4-2 shows hoe the process combines both deductive and inductive elements.

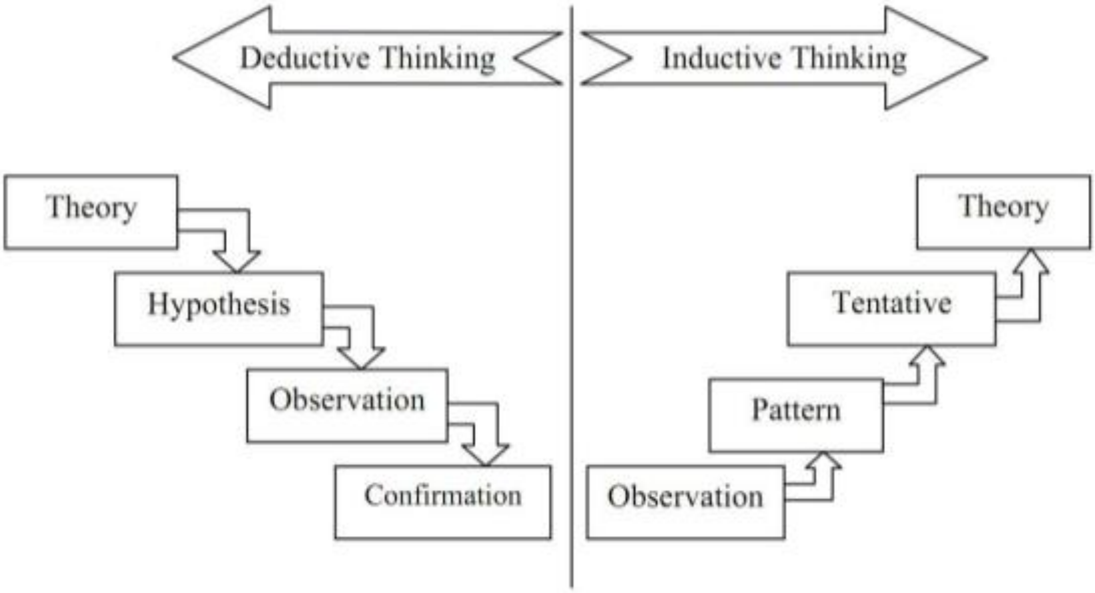


Figure 4-2: An abductive approach
Source: Bryman and Bell (2015)

This thesis, following the abductive approach, begins with research a question where existing theory is less accounted to provide answers (Bryman and Bell, 2015, p. 27). The past literature could not provide sufficient evidences to evaluate what is working in the security profession and what does not seem to be providing benefit with respect to knowledge to address and mitigate identity theft. There are few studies which focused on the extent to which companies are willing to share fraud related knowledge (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Feledi, Fenz and Lechner, 2013). It is also explored superficially whether knowledge shared through online forums is able to reduce risk of identity theft (Tamjidyamcholo *et al.*, 2014). Behavioural reactions to the knowledge sharing process require further investigation. These phenomena are explained in Chapters 2 and 3 with respect to knowledge sharing practice in online retail. Therefore, abduction approach is applied to guide better understanding.

4.4 Research Strategy

Social scientists rely on either quantitative or qualitative methods or they combine them to conduct their studies depending on the nature of the topic (Bryman, 2012; Somekh and Lewin, 2005; Newman, 2005). The quantitative methods are useful to test the statistical model designed using existing theories. Qualitative methods seek to pay attention to contextual details wherein more limited but more intense work is carried out (Peng and Sutanto, 2012, p. 146). Easterby-Smith, Thorpe, and Jackson (2012, p. 159) noticed that, "*Qualitative research is [a] creative process which aims to understand the sense the respondents make of their world*". This is similar to Silverman's (2005, p. 34) recommendation that "*if you are concerned with exploring people's life histories or every day behaviour then qualitative methods may be favoured"*. An inter-organisational knowledge sharing process is deemed evaluative by employing qualitative methods (Flores, Antonsen and Ekstedt, 2014; Easterby-Smith, Lyles and Tsang, 2008). Easterby-Smith, Lyes and Tsang (2008) reviewed a special issue on Inter-organisational Knowledge Transfer in the *Journal of Management Studies*. They found that a qualitative research approach is useful where an inquiry involves investigating knowledge sharing processes. Knowledge sharing processes evolve over time with the use of efficient communication environment to better exchange knowledge and information among the knowledge holders.

Quantitative methods such as surveys are not effective in exploring the richness of security officials' knowledge sharing activities, because it involves behavioural factors (Flores, Antonsen and Ekstedt, 2014). Pérez-Nordtvedt *et al.* (2008, p. 738) suggest that, *"A survey-based approach to measurement cannot fully capture the richness and social complexity of knowledge transfer process*". Based on these suggestions, this study employs qualitative methods to inquire into the topic. Qualitative techniques are primary means of conducting social science research (Denzin and Lincoln, 2011; Gummesson, 2000), which falls into narrative, phenomenology, grounded theory, ethnography and case study (Creswell, 2013). These are explained below.

4.4.1 Narrative Inquiry

According to Paley and Eva (2005, p. 83-97) narrative inquiry relates to a sequence of events to create causal claims. These claims may be true or false and they can be tested. A narrative organises various events constituted in a way to elicit a particular effect. Such effect can distract attention away from new surprises and make implicit claims about causation. A narrative inquiry focuses on how "*participants can best be accessed by collecting and analysing these as complete stories, rather than collecting them as bits of data that flow from specific interview questions*" (Saunders, Thornhill and Lewis, 2015, p. 197). This study seeks to evaluate knowledge sharing processes in the online retail business to understand the wider context. Therefore, narratives inquiry may not provide rich explanation of designed research questions, because it mainly focuses on one to two storytellers (Paley and Eva, 2005, p. 83-97).

4.4.2 Phenomenology

Phenomenologists believe that essential truth about reality is grounded in people's experiences that can be uncovered through investigating subjective phenomena (Rolfe, 2006). This is similar to the thinking of Nåden (2010, p. 80) based on Gadamer's philosophy that "*resonance of the meaning goes beyond what is said*". Phenomenology focuses to uncover meaning that is hidden in the text (Lewis-Beck, Bryman and Liao, 2004, p. 454). The focus is placed to understand life from life. The phenomena that this study seeks to explore are not completely hidden or forgotten, but remain unexplored.

4.4.3 Grounded Theory

Initially grounded theory was designed to inquire in the medical field; however, since then it spread to other disciplines (Glaser and Strauss, 1968). The purpose of the grounded theory method is to produce theory induced from a set of data (Saunders, Thornhill and Lewis, 2015). Knowledge sharing is not a new phenomenon; the context in which this study takes place is new. Theory generation is not the only aim of this thesis because it also aims to synthesise the data collected in association with previous theories.

4.4.4 Ethnography

An ethnographer focuses on cultural endeavours to portray culture in a realistic and enriching fashion in order to convey to the reader the authentic flavour of that culture (Basit, 2003). Ethnography is a cultural description that allows researchers to explore how individuals structure their world, and it contributes to research using the methods such as observation in a real setting. This strategy contributes data that can easily be quantifiable via documenting and portraying every day experiences of an individual (Creswell, 2013). The inquirer with extensive access to a research site conducts this study. In the current research, it is not easy to approach companies on a regular basis to observe the phenomena. Although ethnography is a useful approach, it may not provide richness about of knowledge sharing behaviours due to accessibility constraints to online retail.

4.4.5 Case Study

A case study is broadly known as "*an intensive study of [a] single unit for the purpose of understanding a larger class of (similar) units"* (Gerring, 2004, p. 342). This study explores organisations that have parallels to other similar organisations. Yin (2009, p. 18) suggests that a case study unfolds two technical aspects. Firstly, contemporary phenomena can be investigated in-depth within the real context. They help to explore the details of a specific phenomenon since it provides a focus-based approach that supports consideration of a situation from many angles (Yin, 2009; Thomas, 2011). For instance, it provides a focus on a single instance whether it is a person, a group, a community or a profession to understand the wider population where it belongs (Basit, 2003). It supports an understanding of the research questions designed based on present time situations (Yin, 2009; 2012), thus it may support investigation into whether elements of knowledge and knowledge sharing employed by the security professionals in online retail advance their learning experience.

Many researchers have employed case study methods in a similar context to explore knowledge sharing behaviour with real actors. Peng and Sutanto (2012) believe that case study design is useful to investigate contextual details within the knowledge sharing process. This allows functional and geographical boundaries. Lopez and Steves (2013) conduct their study on acquiring external knowledge sharing by using a case study design. A case study is a useful strategy for acquiring knowledge to understand an organisation and its working operation (Gummesson, 2000; Hartley, 2004; Stake, 2005). Motivated by these similar studies and the methodological implications of other methods such as surveys, the case study was deemed useful in this investigation. These assumptions are supported by Yin (2009) by explaining the question and its relevance to the case study. Yin (2009, p. 9) advocates two possibilities to use a case study when key research questions contain the 'what' keywords. The first possibility relates to the questions such as research question 1 (RQ1), which seeks to answer, "*What is working for retail sector organisations and what does not seem to be providing benefit with regard to knowledge sharing to address and mitigate identity theft?"* This question matches Yin's criteria of exploratory investigation with a rationale.

Secondly, a type of question with the ‘what’ keyword is mentioned in research question (RQ2), which asks, “*To what extent companies are willing to share fraud prevention knowledge with each other and under what the condition(s)?”* This question advocates the situation when the line of inquiry addresses “how much”. This is more likely to involve surveys. In contrast, the situation comprised of questions such as, research question 3 (RQ3) whereby keyword ‘why’ is utilised “*Why do some individuals either not take part or have less active participation in information security knowledge sharing?”* This is more explanatory and is leaded by the use of case studies. Research question (RQ4) *advocates a situation to explore the best knowledge- sharing framework in the security profession in online retail that facilitates inter-organisational knowledge sharing processes.* Most of these investigations involve the use of case studies.

Case studies concentrate on multiple sources of evidences to converge and triangulate (Yin, 2009, p. 18). These details are consistent with this line of inquiry (column 3 in Table 4-1). A multiple case study approach supports understanding of different associated elements (Yin, 2009). Multiple cases assist in making a logical chain of evidence (Miles, Huberman and Saldana, 2014; Newman, 2005). It helps to “*strengthen the precision, validity, stability and trustworthiness of the findings*” (Miles, Huberman and Saldana, 2014, p. 33). Carefully designed multiple case studies are useful in this line of inquiry (Pérez-Nordtvedt *et al.*, 2008). The choice of multiple cases was also motivated by the nature of the topic. Evaluating the inter-organisational knowledge sharing process requires a minimum of two companies (Easterby-Smith, Lyles and Tsang, 2008). Therefore, the multiple case study design is favoured to study inter-organisational knowledge sharing processes surrounding identity theft prevention and is explained as follows.

4.5 Case Study Design and Data Collection

The design of the cases was based on the following criteria:

- Access to at least 3-4 online retailers, each with 10-12 interviews and internal documents
- Companies should be UK based
- The companies should be medium to large organisations working with information systems under their control
- Be willing to participate by providing face-to-face interaction

Case study based research can bring many challenges including if the sample is large, the cases can be studied less intensively (Gerring, 2004), whereas if the sample is too small can make justification hard (Siggelkow, 2007). A balanced sample supports efficient illustration and motivation to more refined conceptualisation (Siggelkow, 2007). It also inspires an inductive theory. Therefore, this study designed on sample of four companies (anonymised as ShoppingCo, PaymentCo, TeleCo and NetworkingCo). Thirty participants interviewed and explored 11 internal documents. These four companies provided useful insights for efficient evaluation. The design of the cases in this study reflects the procedures identified by Yin (2009, p. 27). Similar to Yin's criteria, secondary sources such as academic literature and published reports were synthesised to identify research gap. As a result of this evaluation, key research questions were designed (Chapter 1, Section 1.3). Further elements of design are explained below.

4.5.1 Research Site

The following criteria were designed to select respondents for this study. Firstly, participants must be working in the online retail sector. Secondly, they must be based in the UK. The UK is chosen to conduct the study for two main reasons. First, it is rich in providing online shopping, since the UK is the Europe's leading online shopping economy (Khan, 2015). The second is that these companies were approachable because the researchers were based in the UK. Because the UK is fourth most prone country to identity theft (Trustwave, 2013, p. 9), officials working in these organisations deemed more engaged in day-to-day fraud prevention activities. Security officials seem knowledgeable to respond research questions adequately. This criterion is similar to purposive sampling followed by Miles, Huberman and Saldana (2014) and Newman (2005) that qualitative samples tend to be purposive if an inquirer selects research site that best suits the nature of the topic. Purposive is a judgemental approach that help researcher to select field that fits the research inquiry (Saunders, Thornhill and Lewis, 2015, p. 284). This technique also supports researcher to seek out from the participants' deliberately and is helpful if the nature of the sample is not clear (Lewis-Beck, Bryman and Liao, 2004, p. 884).

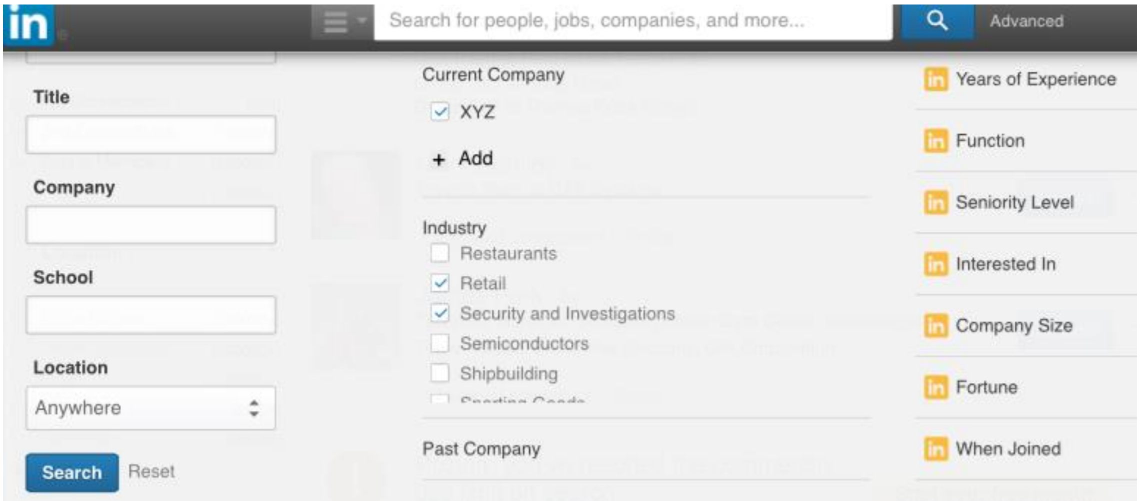
However, convincing participants was a major challenge due to involved organisational complex issues, managerial concerns and political matters. To overcome these challenges, Easterby-Smith, Thorpe and Jackson (2012, p. 3) have advised to consult senior management before approaching the operational staff (Easterby-Smith, Thorpe and Jackson, 2012, p. 3), because they have power to allow enquirer's access to the company and its officials. Saunders, Thornhill and Lewis (2015, p. 378) also agree that the person in-charge in the organisation is more likely to involve if "*the interview topic is seen more to be interesting and relevant to their current work*". Based on these suggestions, invitation letters were dispatched to the companies that introduced nature of the topic, problem of identity theft within online retail and outweigh benefit to the management from their participation (Appendix 1).

An initial entry was gained through academic discussion. ShoppingCo was accessed with the help of university-industry research collaboration. Marshal and Rossman (1995) and Denzin and Lincoln (2011) have advised to learn from an opportunity. Snowballing facilitates access to informants through contact information given by already recruited participants (Noy, 2008, p. 330). This allows identification by participants already enrolled of other members of the same or different groups (Lewis-Beck, Bryman and Liao, 2004, p. 884). Snowballing is useful to generate inductive theory (Miles, Huberman and Saldana, 2014). Initial entry was used to access more participants from ShoppingCo. Snowballing was also used to access other companies. Participants from ShoppingCo and TeleCo referred their colleagues. Thus, eighteen participants in ShoppingCo and seven in TeleCo were accessed using snowballing. ShoppingCo2 and PublishingCo mentioned in Figure 4-6 were also accessed by the recruited peer organisations. However, since only one interview was possible from these two companies, therefore, these were considered as mini cases and were discarded.

To access more participants, LinkedIn professional networking site was used to search relevant audience (Figure 4-3). An advanced search criterion was applied to find the companies and the industry in which informants work. The well-known online retail organisations were invited via an email attachment. Over 300 participants were approached but only five participants from PaymentCo and NetworkingCo 2 agreed due to the sensitivity of the topic.

The special focus was given to fraud, risk, IT-security and compliance officials due to their knowledge and expertise in the information security. LinkedIn groups such as *Fraud Prevention Network*, *Anti-Fraud experts*, *Information Security Community*, and *UK Loss Prevention* were joined to access relevant participants. This technique reflects Flores, Antonsen and Ekstedt (2014, p. 93) advised that:

> "*In information security contexts, generation of knowledge can be manifested through information security specialists being hired to perform activities that increase information security knowledge, or having dedicated units within the organization that are responsible for those activities*."



Title:

Company:

School:

Location: Anywhere

Current Company
☑ XYZ

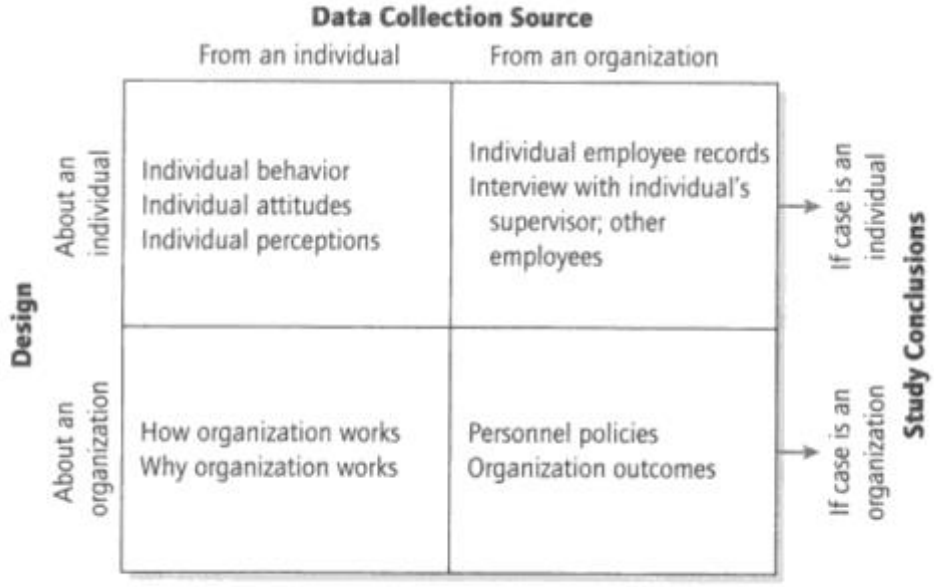
Industry
□ Restaurants
☑ Retail
☑ Security and Investigations
□ Semiconductors
□ Shipbuilding

Figure 4-3: LinkedIn search for relevant participants

A key aspect of site selection is convenience, i.e. "*easy access to the research site*" (Marshall and Rossman, 1995, p. 51) both geographically and immediately (Miles, Huberman and Saldana, 2014). Therefore, companies based in the Northwest of England were selected. Out of 32, only five participants were based in the Southeast and the rest were from the Northwest.

4.5.2 Unit of Analysis

This study considered online retail as the unit whereby special focus was given to the teams engaged in information security. Yin (2009) suggests that evaluation of previous theories, units of analysis and the data collection protocols guide empirical data collection efficiently. Figure 4-4 shows the units of analysis.



Design	Data Collection Source: From an individual	Data Collection Source: From an organization	Study Conclusions
About an individual	Individual behavior Individual attitudes Individual perceptions	Individual employee records Interview with individual's supervisor; other employees	→ If case is an individual
About an organization	How organization works Why organization works	Personnel policies Organization outcomes	→ If case is an organization

Figure 4-4: Units of analysis
(Adapted from Yin, 2009)

Figure 4-4 reflects the situation associated with organisational and individual characteristics. Organisational characteristics such as fraud prevention tools and techniques, security operations, efficient communication and frequent collaboration can examine what is working in the organisation. This aspect reflects bottom-left box (Figure 4-4) which evaluates how organisation works. Individual responses were required to evaluate motivation, incentives, abilities, trust and willingness to share their learning experiences. The individuals' response reflected in top-left box which evaluates behaviour, attitude and perception. This criterion was also followed previously (Miles, Huberman and Saldana, 2014) whereby researchers explored imprisoned suspects and their booking arrangements. They interviewed all people involved such as police, suspects and attorneys. They also observed phenomena in person and collected relevant documents.

Similarly, knowledge sharing practice requires multiple units of analysis whereby each organisation is analysed to consider individual and organisational outcomes. In doing so, exploring organisational information security policies and practices to prevent identity theft and asking whether company resources and capabilities were effective in exploring external knowledge. Therefore, considered both, the identity fraud practices and organisational abilities to explore external knowledge. The other aspect such as how their members of staff involved in this profession react to the knowledge sharing process required a direct mode of communication with the staff. Both aspects were considered in the design: information security department (their abilities and recourses, policies and practices) and the individuals' behaviours, attitudes, perceptions, trusts, and fears of the knowledge sharing process. An individual aspect considered opinions from real actors. This helped to address RQ2 and RQ3 whereby individual behaviours, perceptions, and attitudes were required. The members closely related RQ1 and RQ4 to organisational abilities aiming to gain an external knowledge and its utilisation.

4.5.3 Interview Design

Interviews are valuable sources when an inquirer seeks experiences of participants (Kumar, 1999). It is purposeful interaction with participants and the purpose is to gather valid and reliable data that answers the research questions adequately (Saunders, Thornhill and Lewis, 2015). Three interview designs are available: unstructured, semi-structured and structured (Saunders, Thornhill and Lewis, 2015, p. 374), and this study adopted a semi-structured design. Semi-structured interviews bring a number of benefits based on the topic. Firstly, the topic considers a specific research area rather than a general discussion, which requires unstructured discussion, whereby a talk may have no specified boundaries (Easterby-Smith, Thorpe and Jackson, 2012, p. 136). Secondly, the research area is relatively new; therefore, it requires an in-depth investigation. A structured interviews design is fixed whereby pre-coded questions and answers are followed that limits exploration (Ryan, Coughlan and Cronin, 2009). This study is explorative and requires discussion with security professionals and involves participants' opinions based on their learning experiences. The semi-structured interview design considers a pre-defined set of questions with a motivation to omit existing questions or ask new ones depending on responses (Saunders, Thornhill and Lewis, 2015). Semi-structured interviews are helpful in an inquiry where either the context is unclear or confidential (Easterby-Smith, Thorpe and Jackson, 2012). Both of these elements are consistent with the present study. Firstly, there is limited empirical literature on the information security knowledge sharing research in the security profession. Secondly, identity theft is a sensitive topic involving discussion of business operational information consisting of customers' details, financial transactions and organisational abilities related to prevention. Therefore, a semi-structured protocol is designed as explained in Appendix 2.

In terms of practicality, the following procedure was employed. Figure 4-5 shows one-to-one and one-to-many interview techniques. Each has its own pros and cons.

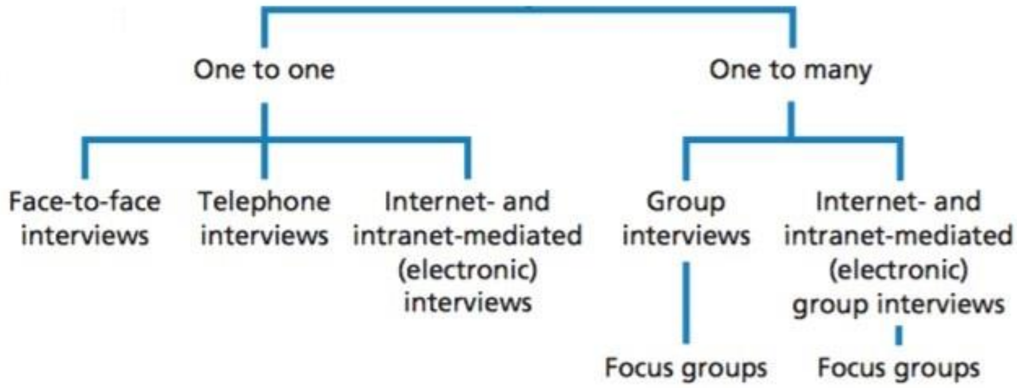

One to one
One to many
Face-to-face interviews
Telephone interviews
Internet- and intranet-mediated (electronic) interviews
Group interviews
Internet- and intranet-mediated (electronic) group interviews
Focus groups
Focus groups

Figure 4-5: Forms of interview design
(Adapted from Saunders, Thornhill and Lewis, 2012, p. 375)

Group interviews technique such as focus groups is useful in saving time and the cost of traveling. This technique was utilised in the similar studies (Ahmad, Maynard and Park, 2014; Elyas *et al.*, 2015). However, a major disadvantage of group interviews is that finding real facts based on accurate information relevant to experiences and attitudes in the presence of number of participants could be distracting. Ryan, Coughlan and Cronin (2009, p. 309) state that this may not facilitate the exploration of participants' perceptions, understandings and experiences. Knowledge sharing is a behavioural concept and a personal opinion was required from the participants depending on trust, relationships and value gained from the knowledge. In the group interviews, the participants may seem reluctant to share their personal opinion in front of others. This study chose to explore the online retail industry. Bringing participants from the security profession under the same roof in this industry was difficult. Therefore, one-to-one interviews were conducted.

Figure 4-5 shows three choices to conduct one-to-one interviews. This study chose face-to-face interviews. The face-to-face provides an environment to observe participant through body language, facial expressions and eye contact. This enhances interpretability of a person's response (Ryan, Coughlan and Cronin, 2009).

Interview Protocol

The design of the interview protocol was based on the research aims and objectives on key research questions. Previous theories guided the design of the research instrument, and protocol was mapped onto the research objectives (OBJ1-OBJ5) and the key research questions (RQ1-RQ4) are explained in detail in Appendix 2.

The interview protocol began by asking demographic questions and the purpose was to initiate a comfortable environment for more fluid interaction (Block #1). These questions are simple one in which the participant's role and responsibilities were addressed. The interviews were started with simple questions that were useful to build interviewee trust for the forthcoming set of complex questions (Ryan, Coughlan and Cronin, 2009). Interviewee and interviewer need to be comfortable (Rubin and Rubin, 2011). To facilitate the environment, simple questions were designed on Wilhelm's (2004, p. 9) seven stages of the fraud management life cycle. This technique helped to explore each participant's roles and responsibilities. Questions from Block #1 were explicitly designed to achieve OBJ1 and explored various fraud prevention measures. These questions also contributed to OBJ4 and OBJ5 where an element of the conceptual framework associated with the participants' nature of knowledge is discussed (Chapter 3, Section 3.5).

Block #2 to Block #6 was specifically designed to address OBJ4 and OBJ5 through the exploration of inter-organisational knowledge sharing practice and a synthesis of frameworks. However, each set of interview questions addressed different key research questions (RQ1- RQ4). For instance, from Block #2, QNo.5 addressed RQ2 which seeks to find the extent to which partnership works between the organisations and the conditions that support partnership collaboration. From the same block QNo.6 contributed to RQ1 that seeks to address what is working for retailers from subscriptions to established fraud forums. Similarly, QNo.7 concentrated on RQ3 which evaluates officials' motivation (or lack thereof) to contribute to participate in virtual communities. A construct associated with members' behaviours concerning performance limitation hurdles knowledge sharing and the collaborations were assembled in (Block #4, QNo.14).

Block #6 was designed with extra questions that addressed managerial actions such as QNo.1, which was based on Australian and Korean empirical studies, which found that senior managers consider their roles technical, mainly focusing on the maintenance and availability of technology (Ahmad, Maynard and Park, 2014, p. 366). Similarly, Barringer and Harrison (2000, p. 380) explored whether management considers more 'skills development' and the knowledge transfer process rather than considering cost benefit analysis (QNo.3). Managers select their knowledge collaborator (QNo.4). They consider the risk of sharing explicit knowledge such as blueprints or documents (2012; Easterby-Smith, Thorpe and Jackson, 2008).

4.5.4 Pilot Study

A pilot study is a useful approach of assessing the quality of an interview protocol (Chenail, 2011). Yin (2009, p. 92) also agrees that it helps in refining data collection plans based on: "*both the content of the data and the procedure to be followed*". Therefore, pilot study was conducted before visiting companies to assess the content of the interview guide, to assess relevance of questions, to ensure the use of simplified language and other practical aspects (such as duration, recording, transcribing). The pilot was divided into two phases. The first phase included distributing a printed schedule among the four senior research colleagues for consultation and followed by discussion. The comments received were implemented in the interview guide. In the second phase, four face-to-face interviews were conducted with four colleagues. During two pilot interviews conducted face-to-face, it was observed that some components needed more depth. As a result, more literature was reviewed to refine research questions and then two more pilot interviews were conducted. The transcript of the first interview was produced and discussed to refine further interview guide for better language and style.

4.5.5 Research Ethics

Moral and ethical considerations are pre-requisites in a study which involves human conduct: i.e. "*First do no harm*" (Miles, Huberman and Saldana, 2014, p. 56). This applies to both the researcher and the researched. The former requires security measures such as familiarity with research site and the people recruited. The latter applies to anonymity, confidentiality and security of the participants' rights. This study followed ethics guidelines produced by the Arts, Humanities and Social Sciences ethics committee at the University of Central Lancashire. The ethical approval was obtained before conducting field visits.

Gaining trust with participants is essential in a study based on empirical investigation such as interviews. It is also advised to consider participants anonymity than the quality of the knowledge produced. However, the truth of unintentional disclosing of participants rights to gain that quality was all that counts (Miles, Huberman and Saldana, 2014, p. 56). Failing to gain the trust can cause exaggerated or fake information from the participants (Easterby-Smith, Thorpe and Jackson, 2012, p. 157). An informed consent section detailing how participants' personal information and company name will be reported in formulating the findings was considered in an invitation letter (see Appendix I). Confidentiality agreements were also signed with ShoppingCo. Participants from other organisations were informed on how data will be collected, saved and used (Miles, Huberman and Saldana, 2014, p. 63). The purpose was to gain trust with associated participants by informing them how the results will be disseminated and what would be the benefit for them from their participation.

Protection of participants' right is a fundamental aspect associated with the interview-based research (Ryan, Coughlan and Cronin, 2009). To consider participants' confidentiality pseudonyms were assigned to each participant and associated company. This is similar to internal documents explored from companies during the field visit. Table 4-3 and 4-4 consider confidentiality and anonymity. However, Miles, Huberman and Saldana (2014, p. 56) raise the question that "*What good is anonymity if people and their colleagues can easily recognise themselves?*" Therefore, interpretation and conclusion checks were performed.

The interviews were recorded in audiotape format. Participants were provided with an opportunity to pause audiotape wherever the interview required any sensitive discussion. Participants were also informed about their right of withdrawal from participation if they feel uncomfortable with the data provided. Audiotapes were transcribed and coded using Nvivo software by manual typing.

Transcription interview tapes was time consuming but useful to data analysis. The interviews were transcribed to evaluate what was said by whom and under which tone of voice (Saunders, Thornhill and Lewis, 2015). Saunders, Thornhill and Lewis (2015) discussed four approaches commonly used to transcribe audio-recorded interviews. The first is to pay a touch typist. Paying a touch typist could be expensive and prone to breach of the confidentiality agreement signed with the companies. The second is the use of voice recognition software that converts a voice into text. It is prone to noise problem due to different dialects, pitches and non-vocal. The third approach is based on the suggestion to use data sampling whereby only the part of the speech that is deemed useful is transcribed. It is difficult to decide what part could be useful for analysis. This study considered a start-play-stop-play mechanism. This process is time consuming, however, it is useful in providing a rich understanding of the data collected and facilitated an early understanding of the themes generated. The transcriptions were cleansed and reviewed to reduce errors. The non-verbal clues from the interviews such as laughs and pauses by participants were also transcribed.

4.6 Data Analysis Procedures

Yin (2009) suggests that units of analysis need to be same as the study question(s). This facilitates a comparison and contrast with previous theories and literature. Transcript summaries (coding and interpretation), reflective diaries and self-memos support data analysis (Saunders, Thornhill and Lewis, 2015). In soft-copy transcript Word documents, new comment technique was used to assign code and interpretation to a chunk of data. This is similar to transcript summary whereby data was first condensed and long statements were briefed (Saunders, Thornhill and Lewis, 2015, p. 576). A snapshot of this process is provided in Appendix 4.

4.6.1 Qualitative Coding

The coding criteria used in this study reflect Saldana's (2009). This study aimed to evaluate inter-organisational knowledge sharing practice in the online retail sector surrounding identity theft. The interviews were conducted to explore data surrounding knowledge sharing framework from Chapter 3 and security measures from Table 2-3. The purpose was to synthesise components of the framework in the security profession. This study aimed to propose an extended framework in the security profession. Therefore, themes were drawn from theoretical framework. However, this study does not limit to already identified themes. New themes have also been identified from the interview data, which in turn support induced theory (Miles, Huberman and Saldana, 2014). These themes were based on repetitive patterns coming from the data such as covert security operations and police-retailer relationship. The data has been categorised to facilitate analysis (Appendix 3).

Each transcript was read and re-read, and then coded with interpretation (Saunders, Thornhill and Lewis, 2015). This technique was applied to both printed transcripts as well as soft-copy Word documents. In Word documents, 'insert new comment' technique was used as self-memos practice. The assigned codes were drawn based on both, theories and data driven. Theory-driven codes were generated from themes discussed in the literature (Chapter 2 and Chapter 3). Themes identified (Table 2-3) were used as deduced code from literature. This is particularly related to the first research objective (OBJ1) which aimed to explore identity theft prevention measures. Similarly, to address research objectives (OBJ4 and OBJ5) themes identified in Chapter 3 is considered which is based on conceptual framework. Data driven codes are provided in Appendix (3) with a hierarchy of coding manual. It also shows pre-identified codes.

4.6.2 Criteria of Interpreting Empirical Data

Nvivo 10 software package is useful for analysing qualitative data. It provides automated coding techniques. However, unlike statistical analyses these outputs cannot be used as final conclusion. It need further description. Yin (2009) describes that a minimum condition of case study based research is dependent on verbatim records. An evaluative explanation of a case is underpinned to response research questions. These analysis requires human analytics such as, "*thinking and listening to how texts speak*" (Smythe *et al.*, 2008, p. 1389).

The Nvivo software package however facilitates pattern-matching with the frequency of the codes repeated. Two rounds were used to analyse the codes. The first is self-analytic strategy utilised through matrices, tabulation, flow chart, and graphics (Miles, Huberman and Saldana, 2014). Figure 5-1, Table 5-1 and Table 5-2 are evidences of this analysis. The second round took place based on a discussion to explore why a particular pattern occurs frequently. This process assisted comparison with previous literature and post analysis thinking.

4.6.3 Logical Linking Criteria

Yin (2009) has discussed two main logical models: (1) individual - traces behaviour taking place in an individual’s mind in the organisation, and (2) organisational - traces events taking places in an individual organisation. Both, individual behaviour, and organisational events are considered in this research cases. Each case firstly explains the identity theft prevention process that basically concentrates on security operations, measures, events and involved stakeholders. Secondly, it explains a knowledge sharing organisation as a whole and the experience of an individual within it.

4.7 Summary of the Field Visits

Participants were selected at various management levels ranging from top to middle management and then individuals performing security-related activities. This criterion allowed assessment of the power and powerlessness of the participants at various management levels associated with knowledge sharing decisions. Respondents were also selected based on their activities. The focus was placed on information technology personnel and on other relevant staff such as, those involved in risk, compliance, and fraud prevention teams. The background of some participants belongs to core technical areas such as IT security professionals, while others were field-based investigators. Some of these participants were engaged in the security professionals’ skills development programs to ensure security awareness culture inside organisations (i.e. eLearning programs and in-house awareness programmes). Some members from networking forums were also interviewed because they are engaged more than these companies in providing the networking facilities and the fraud prevention knowledge base to control identity theft. Although these networking companies are not online businesses, however these organise meetings for online fraud departments from retail sector organisations and these are in a position to see the dynamics of the online interaction. Data was collected from four companies and the methods of data collection are summarised below (Table 4-2).

Table 4-2: Case study companies' size

Company	***Staff***	***Methods***	***Enterprise***
ShoppingCo	Over 4000	Interviews, informal discussion, field notes, internal documents, observations	Large
PaymentCo	Over 1000	Interviews, formal discussion, field notes, internal documents, observations	Large
TeleCo	Over 100	Interviews, informal discussion, field notes, observations	Small to medium
NetworkingCo	Over 40	Interviews, internal documents, observations	Medium – based on the purpose

Table 4-3: Company and participants' codes

Company Code	***Serial***	***Participants' Code***	***Participants' job Role***
ShoppingCo	1	"Jon"	Senior manager
	2	"Bram"	Senior manager
	3	"Celia"	Auditor
	4	"Sam"	Senior manager
	5	"Greg"	Senior manager
	6	"Freddy"	Senior manager
	7	"Adie"	Analyst
	8	"Lyn"	Analyst
	9	"Ronny"	Analyst
	10	"Pat"	IT Security Specialist
	11	"Mandy"	Middle manager
	12	"Fran"	Identity theft Adviser
	13	"Drew"	Identity theft Adviser
	14	"Bella"	Identity theft Adviser
	15	"Debra"	Senior manager
	16	"Carl"	Head of Physical Security
	17	"Opt1" Technical surveillance counter measures	Explained by Technical Security Manager
	18	"Opt2" Operation Managed Delivery	Briefed by a groups that performs security operations
PaymentCo	19	"Jackson"	Senior fraud and risk specialist
	20	"Pon"	Manager compliance
	21	"Fredrick"	Director card services
NetworkingCo	22	"Sophie"	Financial Crime and Intelligence, Deputy Head
	23	"Ben"	Financial Crime Intelligence Manager
TeleCo	24	"Gizmo"	Data Manager
	25	"Happy"	Head of IT
	26	"Jessie"	Business Recruitment Director
	27	"Mac"	Head of Quality and Compliance
	28	"Nickel"	IT Support
	29	"Oliver"	Outbound Agent
	30	"Preston"	Training and Compliance Manager

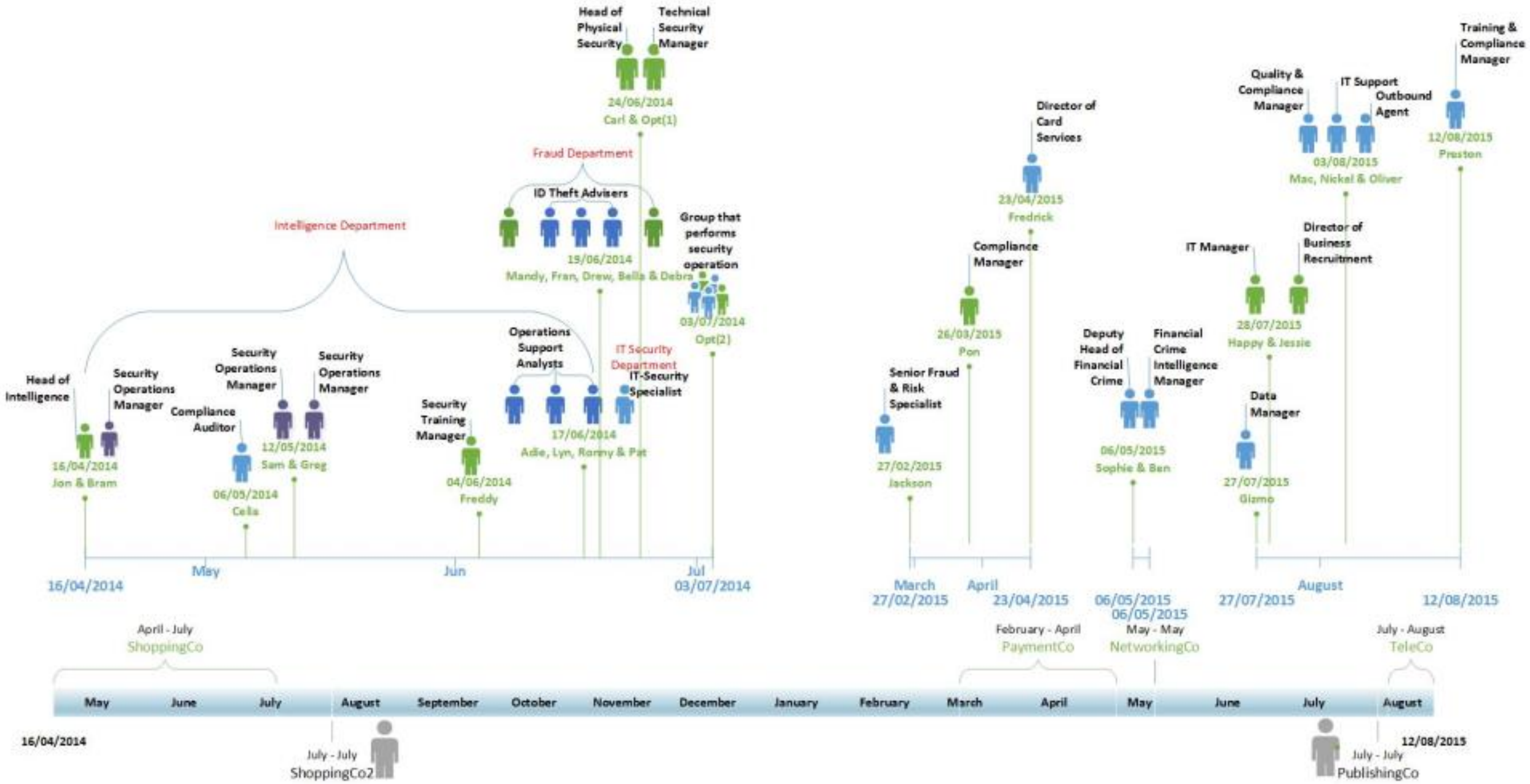


Figure 4-6: Data collection timeline and field visits

Figure 4-6 illustrates field visits by identifying the timeline, the participants, and their roles. The first investigated company was ShoppingCo. Field visits within this company consisted of 16 face-to-face interviews and 2 practical briefings covering how security operations are performed. The data from this company was collected from May to July 2014. The field visit began by interviewing the intelligence department whereby three security operation managers and a head of intelligence were interviewed. It also collected data from a member of compliance team, one training manager, and three operations support analysts. One participant from IT-Security was interviewed same day as operations support analysts. Five participants from the fraud department, two middle managers and three identity theft advisers were also interviewed. A head of physical security was interviewed as well. ShoppingCo briefed two security operations: first was led by a technical security operation manager (Opt1), whereby it was discussed how latest technology prevents identity theft. The field study was concluded with a second security operation (Opt2) briefed by a group that performs covert security operations.

ShoppingCo2 was then investigated and ended up with only one interview with the head of security in July 2014. The company was approached with the help of ShoppingCo by using a snowballing approach. Initially they agreed to provide access to at least 10 informants. However, they changed their mind for several reasons. Firstly, from University of Central Lancashire three researchers approached the company at same time. Because in the retail industry time is precious, therefore, they were unable to decide which investigator should be given an access. Secondly, they were concerned about the sensitivity of the research topic which involves company’s performance and sensitive data such as, customers’ information. Direct invitation was also sent to others at least more than other 20 informants with a number of reminders. Nevertheless, it appeared to be with no fruition.

PaymentCo was visited next from February to April 2015, three interviews were conducted, and internal documents explored. The first interview was conducted with a senior fraud and risk specialist. This was followed by a compliance manager and finished up with a director of card services. Similar to ShoppingCo2, at least more than 20 participants were invited and reminded for an interview. Snowball was also applied, with no fruition though.

Next, NetworkingCo was investigated with two officials on the same day in May 2015. The first participant recruited was the deputy head of financial crime and the second was financial crime intelligence manager. The nature of the company was elaborated sufficiently with two participants as they provided rich information on how networking facility was used by the retailers to reduce identity theft risk.

There was one interview with PublishingCo with the director conducted in July 2015. The company was small. They were also failed to show knowledge intense activities such storage and retrieval, or gaining knowledge from other peers. Even though they were online, they had no fraud related staff. As a result, it was discarded from further investigation.

The data collection process ended with TeleCo with seven officials at different levels from July to August 2015. In Figure 4-6 above, the participants from ShoppingCo2 and PublishingCo were also discarded due to very limited access.

Documents collected in field are summarised and coded (pseudonyms) as follows.

Internal Document Codes

Table 4-4: Internal documents codes

Company	***Serial***	***Code***	***Document type***
ShoppingCo	1	(ShoppingCo.Doc1. 2014)	Word document (prepared for talk to explain ShoppingCo.PPT1): Covert Security Operation – a one way forward combating retail crime, presented at Retail Fraud Conference, 2014.
	2	(ShoppingCo.Doc2. 2014)	“Greg’s” think piece, presented at British Retail Consortium Conference
	3	(ShoppingCo.Doc3. 2014)	Word documents (prepared for talk to explain ShoppingCo.PPT2): Fraud Prevention Strategy and involved teams responsibilities. A talk presented at London Crime Scott, emailed to Author
	4	(ShoppingCo.Doc4. 2014)	Covert Operations – the Retail Process
	5	(ShoppingCo.Figure1. 2014)	Group Security Structure
	6	(ShoppingCo.PPT1. 2014)	PowerPoint presentation explains covert security operation – a one way forward combating retail crime, presented at Retail Fraud Conference 2014
	7	(ShoppingCo.PPT2. 2014)	PowerPoint presentation explains security operation and teams, presented at London Crime Scott
PaymentCo	8	(PaymentCo.Doc1. 2014)	Retrieval Request Report – UK policy, a document based on knowledge learnt from Merchant Risk Council, 2014
	9	(PaymentCo.Doc2. 2014)	UK risk monitoring Task list, weekly work schedule
Networking Co	10	(NetworkingCo.Doc1. 2014)	Interactive Datum Newsletter. An internal newsletter shared with members only.
	11	(NetworkingCo.Doc2. 2015)	Confidential Datum Newsletter. An internal newsletter shared with members only.

CHAPTER 5 DATA ANALYSIS AND RESULTS

5.1 Introduction

This chapter reports the results obtained from ShoppingCo, PaymentCo, TeleCo and NetworkingCo. It is divided into four major sections. Each reports findings from one of the respondent organisations. It begins by presenting findings from ShoppingCo. PaymentCo is then reported. ShoppingCo and PaymentCo due to dealing identity details were found more prone to identity theft and related frauds. Therefore, these companies are reported in depth. These businesses had dedicated risk assessment and fraud prevention departments to help address and mitigate identity frauds. TeleCo is a small organisation works for other businesses and holds customers' data. Finally, NetworkingCo is explained as either to support or reject insights from the other three cases by discussing the extent to which online forums are useful to help address and mitigate identity theft. The criteria of analysing results are centred on the research objectives and key research questions. The chapter reports identity theft prevention, and then evaluates knowledge sharing practice in each organisation. Elaborating the major findings concludes this chapter.

5.2 ShoppingCo

ShoppingCo is a multi-brand online retailer listed in the top 50 UK retailers by sales during 2014/2015 financial years. The company employs between 4,000 and 5,000 staff with 80% of its consumers buy products online. It provides consumers with a credit based on 'buy now and pay latter' schemes. Consequently, they are highly susceptible to high loss due to identity theft. As a result, it employs identity theft prevention and other risk assessment related staffs to take proactive preventative measures.

5.2.1 Identity Theft Prevention Practice

In the ShoppingCo, fraud prevention process is central surrounded by four supporting elements to help prevent identity theft. Figure 5-1 shows three major internal (top management, IS teams and fraud prevention) and two external (mobility and external investigative support) sources engaged in the fraud prevention process. Fraud prevention is located at the centre of the organisation connected by top management and internal information security departments. This department also gains support from two outsourcing companies that provide security programs such as anti-phishing and web solutions. This department jointly perform security operations with the police and courier companies. This process is illustrated in Figure 5-1.

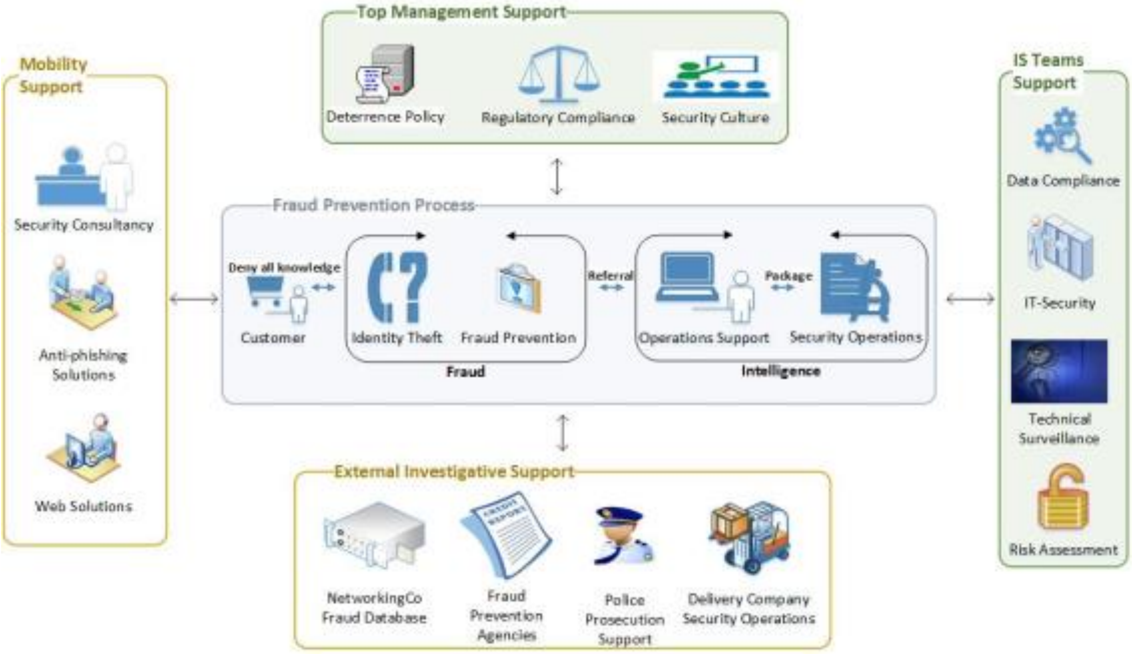


Figure 5-1: ShoppingCo identity theft prevention components

Fraud Prevention Process

Figure 5-1 shows two major teams engaged in the centre of the fraud prevention known as Fraud and Intelligence. The former deals with customers and fraudsters on the phone and the latter finds root causes of committed fraudulent cases to produce legal evidence for prosecution.

Fraud: ShoppingCo identifies suspects using two components. Firstly, customer profiling is implemented using tactics such as flags and alerts. Secondly, a victim informs the company on a phone call. The Fraud team handles these complain from potential victims. This team is consisted of fraud prevention experts and identity theft advisers. The former deals with customer profiling history and the latter deals with complains coming from victims of compromised identities. Customers profiling techniques are summarised in Table 5-1.

Table 5-1: Customer profiling

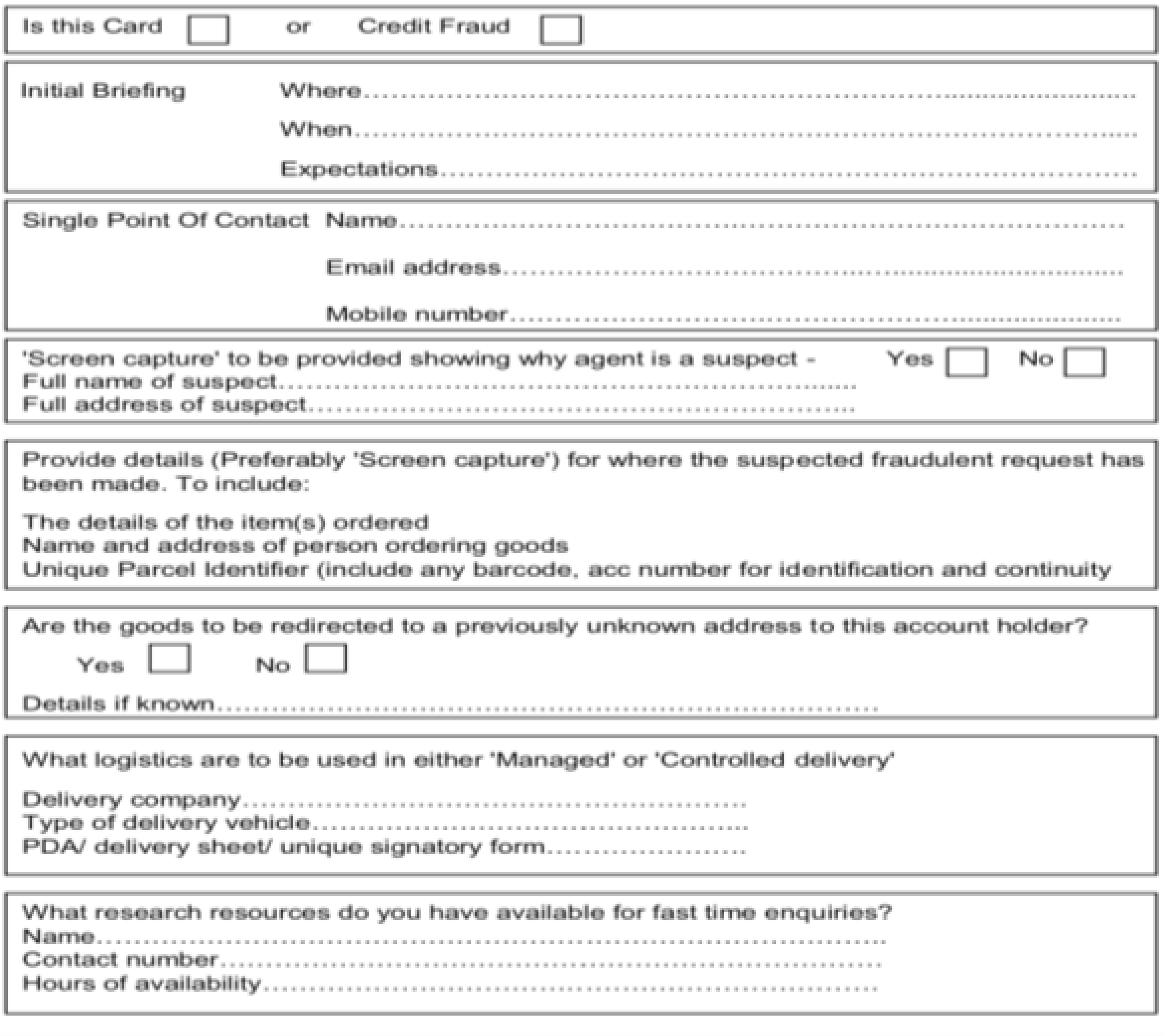
Operation	***Purpose***
Device recognition	"*Cookies*" are stored on buyer's system to identify who are they, which device do they use to prevent loss from same person (the details of this tactic can be found on: https://www.gov.uk/help/cookies)
Password protection	Answering security questions such as mother's maiden name, child hood school and street where they played first helps to prevent account hijack.
Customer spending history	Data mining tactics are implemented to determine how much customers spend normally, how regularly do they spend and their methods of payment.
Identifying limit on the first order	ShoppingCo limits expenditure on first order of its new registered customer to avoid a considerable loss.

Customers' profiling history (Table 5-1) is a proactive process to prevent identity frauds. This involves checking whether the parcel is going to an alternate delivery address. This system looks at whether the item ordered is expensive, or if it is linked to a suspicious area such as the London metropolitan region where most crime originate. ShoppingCo revealed that over 60% of fraudulent cases occurred in London. Therefore, they carefully evaluate address, telephone number and email and match with previous fraudulent cases. In doing so, a device recognition system helps to identify a fraudster if he or she used same device to place an order previously. NetworkingCo also comments on the benefit of using device recognition (Section, 5.3.1). A fraudulent database of compromised identities is checked with their IP addresses. To secure a customer from compromising identities, they implement security questions. The company also limits the first order on newly registered accounts to prevent losing more than a minimum amount.

Customer spending history (Table 5-1) is consistent with "*intrinsic features extraction*" whereby companies evaluate the spending patterns of customers to detect any fraudulent act (Van Vlasselaer *et al.*, 2015, p. 41). Van Vlasselaer *et al.* (2015) have discussed useful components to evaluate customer profiling such as checking frequency of transactions, the amounts normally spend the customer, and time spent since the last transaction. However, these authors focus on a wider context. They covered companies that offer global online shopping. Therefore, many features are inconsistent with ShoppingCo's event occurrence system. ShoppingCo sells products within the UK only. Checking currency, regions and country is not relevant. Customers profiling techniques are also used and discussed by PaymentCo (Section 5.3.1). Van Vlasselaer *et al.*, (2015) deduced from companies similar to PaymentCo discussed in the following section.

ShoppingCo’s reactive process starts when customer telephones to report that he or she has received a letter from the company about unknown online purchases. As evidence, ShoppingCo obtains signed document from them called “*deny all knowledge*”. The purpose is to confirm whether the case belongs to first party frauds, whereby a customer deceives the company by using their own details and after receiving the item, they deny all knowledge. As a result, ShoppingCo either removes fraudulently registered accounts or modifies the details of existing genuine customer. In either situations, they report the case to the database of compromised identities to keep other companies informed from being victimised by the same person. Fraud prevention team forwards *‘referral’* consisting of information such as a name, delivery or IP address to the intelligence team for further investigation.

Intelligence department: The Intelligence team consists of dedicated analysts known as *Operations Support* and field-based investigators to perform *Security Operations* (Figure 5-1). These teams produce legal evidences to present to the court either to recover the assets lost or charge a penalty. Output from this team is a “*package”* that consists IP address, credit history checks, addresses, and other associated information that identify a suspect. To produce this package, they use 192.com to collect address information and Equifax to check a customers’ credit history. The package is then forwarded to *Security Operations* to perform covert security operation jointly with the police to arrest suspects. *Security Operations* is a field based team consists of retired police officers. They are able to gain police involvement. They provide statement of facts, computer screen Google maps, printouts, call recordings and view of delivery address as supportive evidences to the police (ShoppingCo.Doc4. 2014). These details are submitted in the form illustrated in Figure 5-3 to gain help from law enforcement.



Is this Card □ or Credit Fraud □

Initial Briefing Where..

When...

Expectations...

Single Point Of Contact Name...

Email address..

Mobile number..

'Screen capture' to be provided showing why agent is a suspect - Yes □ No □
Full name of suspect...
Full address of suspect..

Provide details (Preferably 'Screen capture') for where the suspected fraudulent request has been made. To include:

The details of the item(s) ordered
Name and address of person ordering goods
Unique Parcel Identifier (include any barcode, acc number for identification and continuity

Are the goods to be redirected to a previously unknown address to this account holder?

Yes □ No □

Details if known...

What logistics are to be used in either 'Managed' or 'Controlled delivery'

Delivery company...
Type of delivery vehicle...
PDA/ delivery sheet/ unique signatory form.........................

What research resources do you have available for fast time enquiries?
Name...
Contact number...
Hours of availability...

Figure 5-2: Managed Delivery Contact Sheet
(Source: ShoppingCo.PPT2, 2014)

External Investigative Support

Ahmad, Maynard and Park (2014, p. 359) discovered that "*In the west, civilian organisations can only apply security strategies at a defensive capacity*". Therefore, they need to use police to take legal actions against the fraudsters. Members from ShoppingCo supported this view as follows:

> *"The retailer must NOT, in any circumstances, insert technical equipment (e.g. a tracker device) into the parcel, without the expressed knowledge and/or authority of police. To do so would constitute a breach in RIPA and contravene the MPS Directed Surveillance Policy [Metropolitan Police Service]."* (ShoppingCo.Doc4. 2014)
> *"As [a] civilian organisation, we have no physical rights to search anyone under law."* (ShoppingCo.Opt1)

External support from police is a prerequisite. Therefore, ShoppingCo reports identity cases to National Fraud Intelligence Bureau (NFIB) by using their channel called '*Action Fraud*'. They also plan covert security operations to trap suspects. Covert security operations are proactive security measures used to arrest identity thieves or intervene to prevent genuine customers from being defrauded.

To perform covert security operation requires Courier Company support which delivers parcels. Covert operation involves tracking devices and geographic zone software. They hide trackers in the parcels going to the suspect's address and record movements by using Gizmo Zone software (Global Positioning System (GPS) tracking).

The covert security operations are useful because it helps to arrest or intervene with the fraudster. It also helps to collect audio and visual evidences useful in the post-arrest investigation process. In collaboration with the police, ShoppingCo have arrested and interviewed a number of suspects to find root causes (ShoppingCo.Doc1, 2014). They are able to understand the ways in which criminals can defraud the companies may help to avoid same suite of threats in the future. Using covert security operations ShoppingCo has prevented frauds worth of millions of pounds and have arrested over 200 identity thieves within eight months (ShoppingCo.Doc1. 2014). ShoppingCo is proud on its intelligence system and human resource. This is evident as follows:

> *"The only time that we believe at case and investigation will be turned down would be for two reasons: First, limited resource or other priorities [by the police force]. Second, the evidence that we suggest is not sufficient for prosecution under the lack of evidence. Those occurrences are very rare on the evidential prosecution side, because our guys are very good at what they do."* (ShoppingCo.Opt2)
> *"They [police force] have been very pleased because of the document that we do… We do professional prosecution files. We just hand the police a very little to do. Others companies do not do that."* (ShoppingCo.Jon)

Top Management Support

Top management supports implementation of several information security countermeasures. Firstly, a deterrence policy helps to prevent internal theft. Secondly, ShoppingCo provides efficient training programs to ensure insider security culture and data preservation. Thirdly, company runs on regulations identified by standard organisations such as ISO. These are explained below.

Deterring internal frauds: Wilhelm (2004, p. 13) asserts that leaders develop security policies to prevent fraud. Elyas *et al.* (2015, p. 77) also support that "*it should be sponsored by senior management*". This study confirms that top management is engaged in policy production. Employees are restricted to access their own devices at certain premises such as shop floor warehouses and datacentres where information system is stored. A participant from senior management evidences this as.

> *"[My] role increased into policies production [and] increased into eLearning program development"* (ShoppingCo.Freddy).

Korean organisations have used non-disclosure agreements, codes of conduct, and penalties to deter staff from stealing customer information (Ahmad, Maynard and Park, 2014). This study however has found use of employment terms and conditions whereby consequences for non-compliance of company rules and regulation is explained. In shop floor warehouses and in the datacentre staffs are restricted to use electronic devices. This is consistent with fear from Bring Your Own Device (BYOD) in the offices (Trustwave, 2013; Bashir and Khan, 2015) which welcomes insider threat of stealing information. This is echoed from a participant:

> *"It is in terms and conditions [for] employment. It sounds rude but you work for us and you go to shop floor, you go to warehouse which has £55 million stock in it. You are not taking your phone. What do you want! A job or to be fired?"* (ShoppingCo.Freddy)

These rules and regulations are not restricted to shop-floor employees only, but senior management also is restricted. They depend upon biometric phone scan and security codes, due to use of confidential information in their devices. In addition, they are bound to use of company owned devices and products which deemed safe rather than BYOD. Senior management has shown trust in Apple Inc. products more than android. This is evidenced as follows:

> *"We find that Android is not as secure as Apple which is ridiculous because we are selling hundreds of tablets per week. And the hackers hack back into us. I don't know what retail industry is doing with regards to tablet security in research and development."* (ShoppingCo.Freddy)

Regulatory compliance: ShoppingCo is efficient to follow governed procedures. Regulatory compliance in the ShoppingCo is twofold. Firstly, they implement law governed by financial service sector such as information security management standard ISO27001. Secondly, they use procedures useful to improve technicalities in the investigation process such as Regulation of Investigatory Power Act 2000 (RIPA). Their data compliance team perform internal and external audits on ISO27001 standards. They need to ensure that they are compliant with customers' information security procedures (Elyas *et al.,* 2014). This is evidenced as follows:

> *"By law under English law and under the financial service sector which is governed by the financial authority, we have to have electronic protection by law, we also have to have electronic protection by association... There is a huge commercial drive when you order mobile, tablet by phone you are borrowing money. Therefore, there is no choice but to invest."* (ShoppingCo.Freddy)

RIPA's[1] procedures are used for robustness and efficiency in producing legal evidence (ShoppingCo.Doc1. 2014). They are not confined to follow RIPA's standards, but they do so for its efficiency.

Security awareness training programs: Value from information security training and awareness programmes was identified (Chapter 2, Section 2.2.3). Special training programmes for employees hired to ensure information security, and a general training for all members of staff to understand the value of customers' information were implemented. ShoppingCo addressed both of these training streams. This is evident from their activities and the training programmes for staff. The participants also identified, for instance:

> *"ShoppingCo has an attitude of serious crime."* (ShoppingCo.Freddy)

They train their security staff to reinforce their information security behaviour and attitude. Special compliance eLearning programmes incorporate data protection

[1] More detail about RIPA can be found on http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

eLearning systems designed for staff directly engaged in data protection. These members take these courses on an annual basis to pass the test. These findings confirm the suggestion provided by an earlier empirical study (Elyas *et al.*, 2015). Elyas *et al.* conducted a study with Australian businesses whereby general mainstreams training was organised for all types of audience. Australian organisations failed to design training programmes specific to employees officially hired to protect customers' data protection. This practice is important to the absorbed knowledge gained from external organisations. Elyas *et al.'s* (2015) participants agreed to the notion that their knowledge is reactive in nature. These officials have advised top management to consider special training courses that enhance their technicalities in a proactive capacity. ShoppingCo addressed training programs that consider the relevant audience and echoed as follows:

> *"In a warehouse environment, you will be trained on security awareness to managers, because even though I am in-charge, this stage is too big for small teams. So what we need to do is to cascade responsibility. So within a warehouse, we would say a key is what training would be benefit from. Say they would be benefit from conflict management. If you do not get conflict, it does in the high street where somebody can come in, like shoplifting and you are in direct conflict. What they would is security awareness [programme] they look for."* (ShoppingCo.Carl)

Information System (internal teams) Support

Data compliance: ShoppingCo uses services from third parties and needs to share its current customer database with service providers to fulfil service requirements. They provide an example of using telecommunication services from one of largest call centres in the world. The data compliance team is composed of field-based auditors. They ensure that the data stored at outsourcing organisations is safe. The auditors not only audit outsourced businesses but also concentrate on the company network. They audit third parties by employing the ISO27001 standard. A participant from the compliance team discusses as follows:

> "*We have [recently] done ISO27001 course. So that is the information security management system. We audit [third party suppliers] against that standard... Any data that is stored and the backup needs to be encrypted, their network and infrastructure needs to be secure"* (ShoppingCo.Celia).

IT- Security: The IT Security team monitors network traffic. The purpose is to confirm that any data or employee details going to third parties is private and transmitted in an encrypted format. If a member of staff emails to anybody by a mistake, they may have no longer access to restricted information. The IT Security team performs activities such as network monitoring, emails monitoring, access management systems, authentication and other IT security related activities. They outsource some work to a company called '*Web Solutions'* (a pseudonym) to facilitate monitoring. Web Solutions provide ShoppingCo with a software package consisting of cloud protection, email analysis and web filter security protection. A participant discusses this facility as follows:

> *"We also have [a] third party email filtering system which is on the cloud. It has recently been taken from the 'Web Solutions'."* (ShoppingCo.Pat)

ShoppingCo also addressed activities which consider implementation of compartmentalisation discussed in (Table 2-2) whereby data is divided and stored into zones. IT security participants restrict or extend staff emails accesses depending on business needs. They also limit software packages used in the communication process at the departmental level. For instance, fraud prevention, business continuity, IT Security and data compliance own their own Yammer groups due to the nature of their work to deal with the sensitive information. Yammer is proprietary social media platform discussed in latter in this chapter.

Technical surveillance countermeasures: ShoppingCo employs sophisticated research tools called '*electronic hostile devices*'. These tools help to detect threat or suspicious activity. They use bug detectors, frequency transmitters, and ultraviolet markers, Delta V advanced range of radio RF bug detector, and module frequency modulators. These tools secure major corporate briefings from industrial espionage. Major corporation meetings were swept using these devices. They also sweep data centres, executive desks, and the fraud department regularly. For instance:

> "*Every month my colleague Ken [pseudonym] and I electronically sweep the executive desks. There are 140 employees in Location3 covering fraud prevention... We sweep that area."* (Shopping.Opt1)

They either put a camera on a bug to identify the suspect or destroy the device and feed misinformation. Their first action is similar to Flayton Electronics (McNulty, 2007) where the author suggests that leaving the vulnerability helps to capture the suspect.

Mobility Support

ShoppingCo uses many outsourcing services including '*Security Consultancy'* (pseudonym) and '*Anti-phishing Solutions'* (pseudonym). Anti-phishing solution is a registered company that has capability to crush out fake website created using ShoppingCo name. This provides ShoppingCo an outsourced built-in solution to help to prevent identity theft. Consultancy helps them in anti-phishing techniques. A participant provides its example as:

> "*Faddy's [Pseudonym] skills regard to hacking and anti-hacking. Faddy gets quality IP and other address information to 'Anti-phishing Solutions' and they have the capability of crashing it out... He is able to get into the underground web sites. It is owned by an organised criminal gang.*" (ShoppingCo.Freddy).

They hire Faddy's skills to identify phishing sites. Faddy's collects information about fake websites created using ShoppingCo's name to fool customers into revealing their personal details and forward it to Anti-Phishing Solutions to cause these fake sites to crash, rendering them inoperative.

5.2.2 Knowledge Sharing Practice

ShoppingCo actively participates at conferences and deliver regular lectures to share their knowledge and experience. Security officials share their learning experience from the security operations (ShoppingCo.PPT1. 2014; ShoppingCo.PPT2. 2014). They describe the roles and responsibilities of various teams involved in identity theft prevention and explain fraud prevention processes (ShoppingCo.Doc1. 2014; ShoppingCo.Doc3. 2014). They not only share this knowledge with peers but also support the police in understanding the nature of the business crimes. They work with many official bodies including the Metropolitan Police, the British Retail Consortium (BRC), the National Fraud Intelligence Bureau (NFIB), the National Crime Agency (NCA), and the Scotland Yard. They are all active in the fraud prevention explained in Figure 5-1. However, ShoppingCo lacks direct collaboration with peer organisations. Several factors discourage this collaboration such as industrial espionage, reputational damage, losing customers going to the rivals, and wasting time on knowledge of low quality coming from other retailers. Since ShoppingCo believes, they are better in the fraud prevention knowledge. They value learning from peers at official forums than direct interaction.

ShoppingCo's knowledge sharing abilities, characteristics, inter-organisational dynamics, and the nature of its knowledge are explained as follows.

ShoppingCo Characteristics

Knowledge absorptive capacity

What is working with regards to knowledge absorbed to address and mitigate identity theft?

ShoppingCo has abilities that inform absorbed knowledge gained from external organisations. Both categories found in ShoppingCo that address knowledge absorptive capacity (Figure 3-4). They appoint experienced professionals and provide a series of in house on-the-job trainings. This is evidenced as follows:

> *"Faddy's skills regard to hacking and anti-hacking is sharp. He is not cheap. He is very short after it. Instead of using him in consultancy, he has now been given full contract and he works directly for the Owners, same as I."* (ShoppingCo.Freddy)
> *"You get training session in here all the time. If a new tools comes in you get trained on it"* (ShoppingCo.Bella)

What does not seem to be providing benefit?

There is lack of trust between members of staff and the top management. There is gap between Spiderman Category A and Category B that links these two categories (Figure 3-4). This will be described later in this section.

Intra-organisational transfer capability -What is working?

ShoppingCo's internal communication mechanisms are summarised in Table 5-2.

Table 5-2: ShoppingCo internal communication mechanisms

Mechanism	***Use***
Yammer	A company owned personalized social media software that updates team achievements (i.e. posting pictures of arrests with associated department). They also use Facebook groups personalised and used within the company.
Shine	Shine is another company owned social media tool used to reward and recognise people within the company who help each other to improve collaboration.
Maximo	IBM's Maximo Asset Management
Telephone conferring	Telephone conferencing is used for inter-departmental communications to explain teamwork.
Email	An email is used to pass work from one team to another.
Microsoft Lync	An online chatting forum used to discuss work and ideas.
Organised trainings	Inter-departmental trainings

Table 5-2 shows that ShoppingCo is fully equipped with abilities to diffuse knowledge to its staff. IT Security officials with core technical abilities use IBM's Maximo to handle security threats. A participant state:

> *"We also have the other way of communicating which is Maximo- it's a way of creating trouble tickets… We use Maximo not just for physical things but also, for example if there is some sort of breach of security which creates an incidence that would also be communicated and recorded within Maximo, that's just one of the tools we refer for communication."* (ShoppingCo.Pat)

Apart from digital mediums, they use offline interactions such as inter-departmental communication. Offline mediums dictate inter-departmental learning. Inter-departmental communication by training is evidenced as follows:

> *"We would show other departments of our company how we do as fraud team, so we would be delivering it to them in August. We are going to do presentation over there to show what the fraud department is all about. So it is within our organisations there are different sites that permanently deal with data collection at LocationX [i.e. call centre team]. It will be myself and a group of 10 of us in the fraud department who will be delivering the session."* (ShoppingCo.Drew)

This statement evidences that they select champions from the teams to spread awareness regarding data preservation to other teams engaged in the data usage. Since the call centre team is directly engaged with customers' data, they consider it necessary to make them aware of its value.

ShoppingCo addressed a few applications that members are encouraged to use (Table 5-2). Yammer and Shine are social media sites used by the company to spread better awareness of the company goals rather than knowledge or best practice. Following statement explains the use of these social media applications.

> *"We arrested someone two or three weeks ago by Greg's investigation. So on Yammer we posted a few pictures of the police man and the parcel and explained what we have done, because there is four and half thousand people at ShoppingCo, and most of them think of the security as a biggest man standing at the door checks who they are as they go through the door. So a lot of people do not actually realise who we are and what we do. Which is a shame because we have a very good security department. I don't think there is many [companies] in the*

> *country that are very close to one that do. So it is used as tool to advertise what we do. But not for exchange of ideas."* (ShoppingCo.Sam)

This statement confirms fears discussed in Section 3.3.2 whereby DiStaso, McCorkindale and Wright (2011) found that members lack control over use of social media application due to criticism from management, negative reaction from colleagues to the content shared and the theft of intellectual property. Since Yammer and Shine are relatively new in ShoppingCo, participants were unable to address how management reacts to the posts that members share. Management, however, addressed distrust in using these tools to share fraud prevention knowledge due to lack of internal trust. Lack of internal trust prevents swift knowledge dissemination among the staff. Knowledge is not adequately shared within the organisational boundaries, therefore, blocks knowledge utilisation. The company is suspicious of employees who can steal intellectual property of the company such as valuable knowledge. This fear is echoed:

> *"Everyone has a Yammer account; we are encouraged to use it. However, we do not talk about security on it. Group security has its own Yammer and is password protected with ID residents only. So we talk about fraud and about financial services only in that approved forum. Otherwise, it is like as if we talking about how many frauds has been done to public. So fraud prevention, business continuity, data compliance, group security, we have our own Yammer which shuts the doors for others. [However], we do not necessarily publish everything on Internet about innovations and ideas such as how we are going to stop this on 'Yammer'. A lot of our staff members are our thieves. Our thieves will use Internet to steal against us and discuss, as they know how to do it. So we have to be careful about how much we give away."* (ShoppingCo.Freddy)

This statement shows that ShoppingCo encourages staff to use social media inside the organisation regardless of whether members belong to top management or individual working in the teams. However, senior management is fearful from its use from the members who can transfer unnecessarily information. They believed that extensive use of communication media could cause to leak important and confidential information. Consequently, internal thieves may steal ideas from the company and sell it to other businesses in exchange for money. This thus limits them to share their knowledge openly inside the organisation. They could not address the use of intranet as a central system that manages security knowledge coming from various sources to share centrally (Flores, Antonsen and Ekstedt, 2014; Argenti, 2013). They could not address in-house employee oriented publication in the security profession (Verčič, Verčič and Sriramesh, 2012). They failed to address any formal mechanism that uses external knowledge to benefit the business. For instance:

> *"I am in very good contact with other companies. About six months ago, I shared those detail with all of my colleagues via emails. I do not know if they spoke to that person or not. No one needs to be that ahead. At least they know that I was there. And in fact when I need to contact someone from other company just recently, I sent an email to my colleagues does any know this [person]; and three people came back that there is the person you need to speak and there is the telephone number. So it is there but not a formal structure I suppose."* (ShoppingCo.Sam)

The above statement states that knowledge and information explored from external sources are not adequately shared within security teams due to lack of formal communication. A communication manager may assist to overcome the gap found internally. There is the possibility that members keep their ideas and feelings from management if it is withholding information from them (Argenti, 2013). Fear from internal investigation also hinders senior management from formal collaboration. Senior management can be against the investigation. The fear from internal investigation is echoed as follows:

> *"No, we don't see each other, because of so why geographically spread. Everybody speaks to everybody on phone daily, emails daily. Skype or FaceTime is better, because there is your body, there is your team, and there is your security group. That is daily, quite frequently, but used with the invitation only. It has to be confidentiality around those meetings, because people are listening. It might be internal investigation. It might be against the very senior person. It happens. We have to be protected, and that is why we have our own separate Yammer, because we cannot share our gripes, our groans, and any great idea, because it is too wider audience. But we use it. Not only Yammer, we have LinkedIn accounts. We are on LinkedIn as well."* (ShoppingCo.Freddy)

This statement reveals several factors. Firstly, it illustrates the kind of favoured technology managers use to contact teams such as Skype and FaceTime. Secondly, it shows distrust on the social media application used for internal communication.

Motivation to teach and learn

Participants suggest that there is no monetary gain in sharing knowledge with peers. However, they value an improved learning process and seek recognition from management. This enhances their level of satisfaction and trust in the company. ShoppingCo is a large organisation and members are situated at various locations. The management through the company owned application such as Yammer and Shine (see Table 5-2) recognises valued staff by posting their achievements internally with comments as follows:

> *"There is no monetary kind of incentives it is just a knowing, breathing and living our values we have got with company a set of values that we do. Idea is to as a business knowing that you are kind of putting and ticking each of those boxes. We have got a new recognition schemes "Shine" [social media application] which has recently been launched just a couple of weeks ago that puts different posts if you spot to one of our values live the purpose so that's our help. I get a lot of personal satisfaction with what I do and you see your team get a lot of flourishing that would be nice… Ultimately to prevent further losses, to ensure we are doing what we need to do let the business progress. We are playing our part as department. When we get the results that motivates me. And knowing my team is doing a good job and helping and supporting. If my knowledge, and all learning I can pass that to help somebody else, that will motivate me to do more."* (ShoppingCo.Debra)

This statement emphasises that sharing team achievements and recognising individual's performances enhance employee satisfaction and improves trust within the company. It is also evident that company owned social media tools are used for posting internal achievements rather than sharing knowledge within the organisation.

Inter-organisational Dynamics

Power Relations

What does not seem to be providing benefit?

Power relation issues exist in ShoppingCo where a win-win situation found as a barrier that hurdles one-to-one collaboration. They supported problem of knowledge asymmetry discussed explicitly in the theory of peer relations in Chapter 3 (Section, 3.4.1). The theory stated that organisations either provide knowledge of low quality or lock-in knowledge within their boundaries. ShoppingCo addressed knowledge lock-in rather than providing knowledge of a low quality. ShoppingCo employees consider themselves as members of a competent organisation equipped with abilities and knowledge to tackle identity theft. Jon and Freddy have stated their views previously that their teams are competent in producing legal evidences to present in the court. In addition, following comments further support their proudness of the power of their intelligence systems.

> "*I think ShoppingCo is leading the way really with regards to the way that we deal with frauds. So they [other retailers] do look to us really for our knowledge."* (ShoppingCo.Bram)

This statement shows that other similar retailers lack the intelligence to tackle the identity theft. Therefore, they depend on ShoppingCo's knowledge. This supports the resource dependence theory discussed in Chapter 2 (Section 2.4). The theory stated that companies extensively depend on input generated outside of the boundaries (Barringer and Harrison, 2000). However, the question is, whether ShoppingCo is competent in the knowledge, unless other organisations of similar nature are also investigated. There is a possibility that the company is more competent than it really is. NetworkingCo has evidence of whether some companies are better than others are and in what sense they are different, since they connect several members and able to see the dynamics operating between the companies (see Section 5.5.1 below). This is assumed that higher position in knowledge possessed by ShoppingCo hinders the formation of strategic alliances whereby staff members from other companies can work together in knowledge exchange relationships as evidenced as follows:

> *"I have never looked at the company and say actually I need to be talking to them. And in the security world if there are many groups as ShoppingCo, more security department like ShoppingCo, it will be very easy to start having a proper collaboration. There is another company similar to ours and they have only one man who covers the whole country. He goes to talk to me (laughs). So [if] there are more companies like ours, I think we can do it better.* (ShoppingCo.Sam)

This statement shows that collaboration is possible when other retailers also improve their intelligence. This statement implicitly addressed their fear from gaining knowledge of poor quality from other retailers due to lack of knowledge resources. They welcome a proper collaboration with a condition of relevant abilities and resources. This statement explicitly answers the key research question RQ2 (b) which was asked to investigate the condition to which companies are willing to share fraud prevention knowledge with each other. ShoppingCo members identified a need, to balanced knowledge from their competitors.

Structures and mechanisms

Partnership:

> *Referring back to literature review, RQ2 (a) was asked to investigate extent to which companies are willing to share fraud prevention knowledge with each other.*

ShoppingCo lacks the desire to address any activity which motivates employees to engage in external communication on a formal one-to-one basis. They can do work-related collaboration with other organisations. Such collaboration however, does not address knowledge sharing elements and is limited to senior management as evidenced from the following:

> "*If we need a help from one of our competitors we ring them inside [by a phone] and ask them we have got a problem in xyz area, have you; yes; then let us meet on a cup of coffee and have a chat. Thus we do not detail out our customers' data*." (ShoppingCo.Sam)
> *"When we feel there is need [to collaborate] we do that, but it is very limited."* (ShoppingCo.Bram)

These statements illustrate a fear of collaboration clearly in unnecessarily disclosing of customers' information. Participants from senior management positions reinforced this fear. Participants collaborate with peers in other organisations to find evidence associated with the identity theft. However, they omit customers' personal details during collaborations. They consider their customers' information as an important asset as echoed in the comments.

> *"Our customers are the data that we have."* (ShoppingCo.Bram)
> *"There is no difference in a warehouse than in the office. Walking out with data of 50 million customers is more dangerous than walking out with 20 carat gold."* (ShoppingCo.Freddy)

ShoppingCo revealed that alliance formation is not useful unless it involves formal contract. Their pre-requisite condition that opens doors for alliances formation is formally signed official contracts among the retailers. This statement answers the condition seeks the study question (RQ2 (b)). They failed to address strategic alliances to learn from different peers. They lack in sufficient trust on a formal basis and support this view as follow:

> *"We have to trust them [first] and we do things on agreements. That is why we as business, and my guys at that meeting was stressing that we*

> *need a department, so that everyone's information goes in that pot. That is where the business world is crying for."* (ShoppingCo.Jon)

This statement is evident of lack of retailers trust in each other and ShoppingCo members assumed superior position hinders knowledge sharing and collaboration. Instead of suggesting one-to-one collaboration, they addressed the use of police as a communication mediator in circulating their knowledge to others as echoed below:

> *"The way forward is not Retail Company talking to Retail Company. The way forward is retail company is telling the police; the police are sharing it with other businesses. It should not be retail to retail."* (ShoppingCo.Greg)

There are two major reasons for trusting police as communication mediator to share knowledge among the retailers. Firstly, police have procedure to grade and sanitise the information. The value of the knowledge and validation of the source are both identified. Recipients can trust shared content. Secondly, companies can make better relationships with the police force. Establishing good relationships with police is their need, because a police unit lacks to deals with business crimes. Retail industry in the UK lacks a dedicated fraud unit, whereas other industries such as banking, mobile, and insurance have their own financial crimes units whereby, they are officially assisted by the police force. As a result, retailers need a close collaboration with the police to deal with business crimes. Trust is an important element in the security profession, as they possess distrustful nature. Even though the use of police as a communication mediator is suggested, however, ShoppingCo is not completely satisfied by its use. The other participant echoed follows:

> *"Now the beauty of the Metropolitan Police is that they are the biggest force in the country. They have forty-three boroughs. So they are splitting to forty-three sections. And they have done a report which is telling everyone in Metropolitan Police on how to investigate Business Crimes. And they have mentioned our company name. So we are quite well thought of within Metropolitan police. It refers to ShoppingCo [and] to other companies. So that is how far we are into them. The City of London Police is responsible for fraud investigation in the whole of the UK except Scotland…. Now similarly they have done the document, which they have circulated outside the Metropolitan Police to the other police forces and when Bram goes to knock on the police doors, that he need assistance; they actually know that we are involved that they have documents from those two forces."* (ShoppingCo.Jon)

Official Forums: Regarding official forums, a gap was found in the literature review and a question was asked whether shared knowledge is able to reduce risk. What is working for the retailers about knowledge sharing to address and mitigate identity theft? ShoppingCo uses online forums to gain an external knowledge (Table 5-3). Senior management is engaged with these collaborations. They attend official meetings organised on forums. ShoppingCo's engaged day-to-day security related working staff advisers, analysts and specialist, however, do not avail an opportunity to attend forums' events and organised conferences to share their learning experience. The following quotations evidence this view:

> *"We do not have any direct contact with external organisations. At my level, I do not. I know a kind of head of our department level- they do site visits and do it at higher level."* (ShoppingCo.Debra)
> *"We do not have any contact with them [CompetitorCo-X, CompetitorCo-Y] as matter of course… That might be a question you better ask to our manager."* (ShoppingCo.Pat)
> *"We have one of our regional manager who attend that meeting and then he feeds that stuff back to us, but we do not deal with anyone from CompetitorCo-X, CompetitorCo-Y."* (ShoppingCo.Adie)

In these statements, most of the interviewees referred their managers' names in external collaboration rather than discussing their own learning experience. These forums and networking structures are summarised in Table 5-3 below.

Table 5-3: ShoppingCo knowledge sharing structure

Structure	***Organisation***	***Reasons***
Online fraud forums	BRC	The British Retail Consortium brings retail companies together. They organize monthly meetings and conferences to discuss and resolve issues in this industry.
	Cifas	Cifas was Previously Credit Industry Fraud Avoidance System (CIFAS) provides a compressive database to subscribers to upload fraudulent information and search fraudulent cases. They also provide networking to facilitate security officials' face-to-face interaction.
	NFIB	National Fraud Intelligence Bureau (NFIB) provides assistance with police to take actions against identity thieves.
One-to-one collaboration with no joint ownership	CompetitorCo-X	CompetitorCo-X is also a financial organisation which offer its customers credit to purchase products from them. Reciprocity is therefore considered.
	CompetitorCo-Y	A neighbour company situated in the same geographic region facilitates more interaction with ShoppingCo.

Forums provide a platform for formal meetings based on monthly, quarterly, and annually. Respondents suggested a number of reasons to use these forums. The most frequently mentioned reason is trust and contractual governance. Firstly, these forums operate on signed agreements. There are rare chances of information leakage. Secondly, they can trust the content shared at these events. Thirdly, using Chatham House Rules whereby members are not allowed to disclose what they have discussed, they run sensitive agenda in these meetings. Chatham House Rules are part of Royal Institute of International Affairs. The rules guide that participants are free to use information received, but neither they identify nor the affiliation of the speaker(s), not that of any other participant, may be revealed. Participants provide evidence as follows:

> *"We have an agreement between ourselves and the companies [on online fraud forums], to share data [and] to sign a document for our own wellbeing."* (ShoppingCo.Jon)
> "*The only sign that we would share information that doesn't breach data protection law is through BRC. We are all [connected] with BRC and it is controlled. This is the success that we are getting out to this particular initiative, certainly, that is shared at the BRC level. But individual case is maintaining confidentiality on the customers as always."* (ShoppingCo.Freddy)

The only member interviewed from ShoppingCo2 provided a different opinion to trust security officials from other organisations as follows:

> *"There are some terms of reference which are pretty clear-cut. We do not breach competition law. We use Chatham House Rules [on these online forums] bearing in mind they come from Police, Military or Security backgrounds. This is not that alien to them. Very few people come to this sort of roles of that background."* (ShoppingCo2.Head of Security)

ShoppingCo members have a little or no collaboration with peers from CompetitorCoX and CompetitorCoY. The only things that connect them with these companies are the similarity in the nature of the work, and geographic closeness. Even though these elements are addressed, they agree that most of their collaborations with peers take place at online fraud forums discussed.

Virtual communities: ShoppingCo participants could not provide answers to low level of active participation. Even though some of them are LinkedIn group members, they do not participate over these forums. Senior management clearly dictate the lack of e-trust. However, other members addressed lack of awareness and lack of time in the use of these applications. They provided their opinion on RQ3 (a) by addressing why some individuals do not take part in information security knowledge sharing. Senior management is reluctant about social media due to security concerns. They believed that sharing best practice on LinkedIn groups is like to giving fraudsters a weapon to attack the company, because it shows their weakest point. They also consider reputation of their company. Leakage is inevitable. They cannot share company woes in public. They believe that these groups are full of vulnerable people due to wider audience consisting of national and international security professional as evidenced as follows:

> *"I have never known anyone been declined… There are certain fraudsters and criminal organised wings siting on these forums to listen to best practices and procedures to get around it… I am happy to share knowledge within the department if its activity, if its criminal methods, or criminal activity oriented, I would not discuss with anyone except my department, because I am giving some one the tools to commit."* (ShoppingCo.Freddy)

There is a limited use of virtual communities by the ShoppingCo analysts, specialists and advisers due to unfamiliarity with LinkedIn groups and their usage to improve knowledge. Evidences provided by these members include an example as stated:

> *"Not then aware of that, but I don't know our manager would be."* (ShoppingCo.Lyn)

There is lack of awareness of relevant online groups whereby security professionals subscribe improvement in their knowledge. There is also lack of motivation. For instance, other participants stated that they have been provided with sufficient knowledge inside the organisation. This would outweigh the benefits of subscriptions to these LinkedIn groups and is echoed as follows:

> *"Because you learn everything here… For my job what I do I do not need to go to anywhere outside. You get training session in here all the time. If a new tool comes in, you get trained on it, so you don't need to do anything else."* (ShoppingCo.Bella)
> *"Different organisations geographically scattered such as TechCo as well. I probably have emails of them I do not choose them as matter of*

> *course. I have so many emails of different outside organisations in a great deal. I do not have a time to follow up. Our business is usually quite intense. We have a lot of work to do in a short period of time and the recourses we have entire recently. Our day is totally taken with business usual the demands of the business. To answer your question, it's not coming out and spend half an hour for example somewhere."* (ShoppingCo.Pat)

Informal social ties: Peers moved to other organisations assist generating informal social networks those support in obtaining an external knowledge from across the organisational boundaries. Among others, Pat provides an opinion as follows:

> *"Now a lot of IT people over those years [have] since moved from ShoppingCo to TechCo* [pseudonym]*. Although they have slightly different regime, because I know these people and they know me, you have the friendship which goes on many-many years. You get information that way as well."* (ShoppingCo.Pat)

These evidences are consistent with the literature discussed in Chapter 2, whereby Almeida, Hohberger and Parada (2011) and Easterby-Smith, Lyles and Tsang (2008) suggest exchanging officials to exchange organisational knowledge. Informal social ties thus are formed by members' exchange. ShoppingCo's IT-Security manager was an example of qualified professional coming from TechCo. A TechCo is renowned IT organisation and world leading company in the IT industry. These findings suggest that ShoppingCo have sources to bring an external knowledge in the form of a member moving to another company or appointing a new member from other organisations. In terms of geographic mediated networks, Jon a senior manager states that:

> *"Head office of CompetitorCo1 is in location-G and the Head office of CompetitorCo2 is just across the road here. Other organisations are scattered around the country, but we have a big coming together at forums, business meetings and business conferences."* (ShoppingCo.Jon)

Trust and Risk

Sensitivity of knowledge – the leakage concerns: participants already addressed issues of leakage of customers' information in the collaboration. Including this, there are many other risks such as industrial espionage and reputational damage inhibit collaboration among the retailers sharing knowledge with peers from other organisations. These are the major concerns at senior management positions. ShoppingCo's participants consider industrial espionage as a major threat whereby rivals may try to steal intellectual property such as ideas and information. ShoppingCo electronically sweep organised meetings to detect any suspicious act. They believe that industrial espionage has been around since people could learn to speak. This is associated with stealing someone's ideas and information. In a briefing during technical surveillance counter measures, they provided example associated to industrial espionage as:

> *"We are talking about multi-million-pound acquisitions. That meeting has to be protected from people who will criminally intrude and sell that information to the rivals."* (ShoppingCo.Opt1)

This statement dictates fear from internal members who could intervene or a rival may send an official to spy information from secure corporate confidential meetings. Reputation is a key to success. Breach of customers' information publicly and rumours of loss published in the news may damage the company's reputation. Consequently, companies lose customers and prevent them from discussing ideas openly as evidenced:

> *"There is nothing going to be personal about it. But what we would not do is to make ourselves foolish either. There is reputational damage to take into consideration. You cannot go into open meeting through all on your woes on the table. That table has to managed and controlled for reputation as well as anything else. It will only be shared at official level and will only be shared with an association [fraud forums] that is deemed safe for reputable by a heads of group security or even at executive level. Not publicly."* (ShoppingCo.Freddy)

The Nature of Knowledge

To determine whether security officials' nature of knowledge is actions oriented that needs more effort to share with others (Panahi, Watson and Partridge, 2013) or the process follows the steps outlined by Nonaka (1994) they were asked whether they require face-to-face mechanisms to clarify receipts what they do. To explore nature of their knowledge, participants were asked about the skills required for their roles and whether experience helps them to perform their tasks efficiently. Asking these questions will help ascertain knowledge can easily be communicated using digital mechanisms. Variety of perspectives was found. Mostly participants supported that they prefer face-to-face mechanism than digital regardless of the nature of their knowledge and the team they are engaged in.

Figure 5-1 shows a number of internal teams involved in the identity theft prevention. Each team consisted of a different set of capabilities and responsibilities. Figure 5-3 below illustrates the nature of the knowledge of each team and its normal day-to-day activities. These teams and their routine work have already been explained in a previous section. To seek the extent of their abilities to gain and absorb new knowledge, they were asked about training provided and whether past experience is useful. One response about the past experience from a member of the Fraud team is that:

> *"I think experience can help. However, we have new staff. So although experience help but you don't have to have experience to do the job."* (ShoppingC.Fran)

This identifies that their work is process-based that uses of a series of steps. This is similar to the responses from the participants belonging to Intelligence departments such as Operations Support, Security Operations, Data Compliance, and Training.

For members working in the IT Security and technical security such as surveillance, the nature of their work is practical, involving the use of technical software and hardware devices. They perform activities like enhancing network security, monitoring emails, monitoring internet access, combatting hacking and anti-hacking, crashing phishing websites, and electronically sweeping internal office spaces. A participant from IT Security elaborates on the team's work:

> *"I just put encryption disk to put some details on. We do encryption, we do email monitoring… we also do internet monitoring – people access to the Internet. We have a Team-G which is filtering system whereby peoples email is restricted or extended depending on business requirement."* (ShoppingCo.Pat)

Technical security is engaged in phishing and anti-phishing, and requires the member proficient skills to perform hacking and anti-hacking activities. There is possibility that members involved in surveillance and IT security are skilled with computing knowledge base. As a result, their knowledge contains elements of high tacitness compared with other teams.

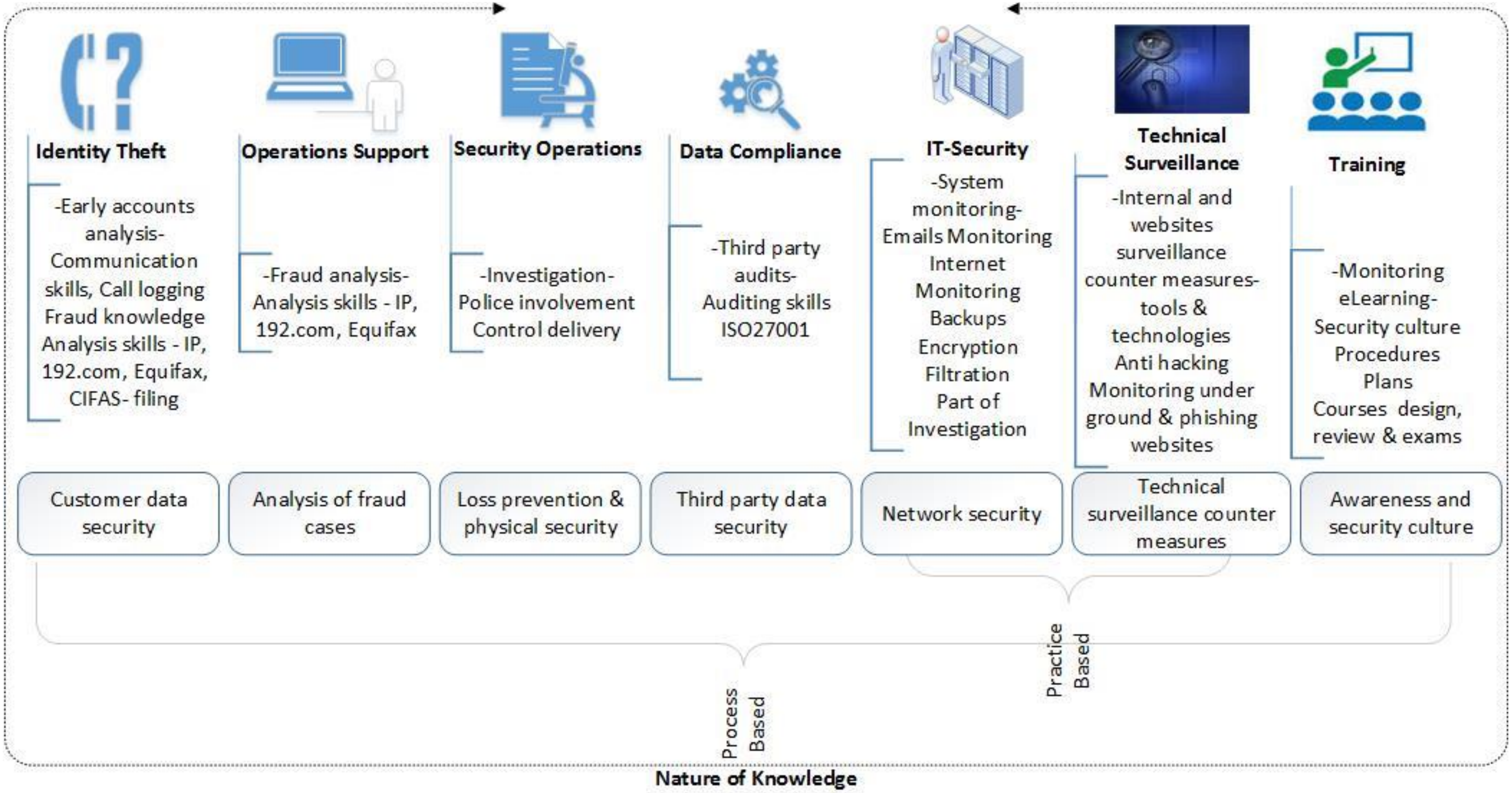


Figure 5-3: ShoppingCo information security teams and their nature of knowledge

Process-based knowledge illustrated in Figure 5-3 may be shared easily with the help of digital mechanisms. However, practice based knowledge may be is difficult to convey message when shared electronically because of high degree of tacitness (Panahi, Watson and Partridge, 2013). This type of knowledge may require face-to-face interactions to convey their message effectively (Nonaka, 1994). Members, therefore, prefer face-to-face interaction to explain what they do and how:

> *"We do face-to-face [interaction] it is easier enough. It is always better discussing, because if you have the question you can get response quickly"* (ShoppingCo.Fran)

One member with a core technical background confirmed that sharing knowledge through social media is more difficult than having a conversation. This is explained as follows:

"Yeah it is difficult. It is better to speak to people. Although we deal with India more on a superficial basis, we don't get in integrity with technical details with them at all." (ShoppingCo.Pat)

5.3 PaymentCo

PaymentCo is a group that sell online payment processing services. Online gambling businesses are its major customers. PaymentCo plays an intermediate role between the banks, merchants and the card schemes (i.e. VISA and MasterCard). They provide customers with a payment facility to purchase and pay with a secured transaction system. They help retailers to obtain a multi-currency system from around the globe. The company serves thousands of businesses and millions of consumers by offering a mobile payment system. They share risk associated with the identity theft in the form of chargeback frauds discussed earlier. PaymentCo therefore has risk analysts and credit check teams to evaluate risk assessment to deal with identity theft.

5.3.1 Identity Theft Prevention Practice

PaymentCo provides two elements of the service such as a gateway service and an acquiring service. A gateway service is provided directly to a customer or to the retailers. It involves processing payment for the merchants. PaymentCo have no liability with the charge of transactions involving a gateway service. In this type of service, they forward card details to the acquiring bank or the card issuer to do checks. Therefore, this element is of low risk to PaymentCo, since it involves financial interaction, there is only processing of the information. The other service is bureau or acquiring service. This service involves a joint liability whereby PaymentCo shares risk with the companies to whom they sell services called merchants. Foreign exchange, e-gambling, binary auction, sports events and music concerts are their common merchants.

PaymentCo supports identity theft definition whereby an owner of the identity defrauds companies using his or her own details. Chapter 2 (Section, 2.2) discussed that merchants are responsible to refund the customer regardless of risk measures taken by them if they request a chargeback (Khan, 2015). PaymentCo provides similar opinion as follows:

> *"We set up payment pages for the merchants. So when the shopper goes to the website and says okay I like that pair of shoes and checks out. That checkout then takes them to the payment page. They would then know the card details. PaymentCo process the information and sends it to the shopper's Card Company or bank. The card company would come back to PaymentCo to confirm and [we] say yes we know them. They are then authorised. If it is not [authorised], we will then send this information back to the shoe retailer. Now say for example this shoe retailer was having financial problems, they could not fulfil the orders,*

> *they could not ship the goods then the person who placed the order will contact the card company and request the chargeback. Now if there is no enough money on their [retailers] account, then PaymentCo could essentially bare that loss. So say for example there is hundred transactions for the one hundred pounds - there is potential loss.”* (PaymentCo.Jackson)

This statement dictates that PaymentCo has a number of threats concerning identity theft. Firstly, customers buying from retailers can defraud. Secondly, there is possibility that merchants themselves could be organised criminals who designed webpages to steal identity details and financial information. Jackson’s explanation confirms Khan’s (2015) definition regarding chargeback fraud whereby consumers defraud companies using their own details. However, an element associated with an intermediate payment service provider was missed. PaymentCo as service provider has risk of financial loss, when merchants are either of fraudulent or financially instable. The amount of loss is also shared by card schemes (Visa, MasterCard and American express). Therefore, risk assessment reports assess merchants’ potential liability, credit checks and transaction monitoring. These strategies help them to cope with fraudulent or high-risk merchants. Merchants prone to identity theft include online gambling and customer services tickets for concert support events. Fraudster can attempt to buy tickets using stolen cards and then they can easily sell. Similar to ShoppingCo, PaymentCo addressed customer-profiling techniques to reduce identity theft as follows:

> *“We are looking at merchants with a high level of refunds, high value transactions, chargebacks, high level of authorisations, velocity which is happening may or may not come across - which is say for example same card used at multiple locations to say- email address used at multiple locations by shoppers. High level of decline, merchants have been inactive for a while – they have not process transaction for a while, somebody put one through somebody called bust out fraud – which is quiet common term in fraud circle where an account is taken over by fraudsters – that account we just set inactive. The fraudsters get hold of the merchants’ identity and start to put transactions. For say if a merchant has not been processing for a long period while we certainly out that transaction, we want to query that and question that. So there is set schedule of work that we look at and work through.”* (PaymentCo.Jackson)

Similar to ShoppingCo, PaymentCo addressed the use of event occurrence matching IP address and transaction monitoring. They consider measuring whether the same card and email account is used at multiple sites to place an order. Customers profiling from

PaymentCo discussed is similar to findings discussed from (Van Vlasselaer *et al.*, 2015, p. 41), since they covered companies offering online shopping globally.

5.3.2 Knowledge Sharing Practice

PaymentCo's participants were aware of their competitors and companies of the similar nature. Officials from PaymentCo interact with peers in networking events such as conferences including events organised for risk related measures. A director of card services details his opinion about the teams those who attend networking events as follows:

> *"I myself don't, however the fraud, risk and compliance [officials] do attend networking events. I meet with directors of other companies to talk about not individual frauds but to talk about high-risk programs."* (PaymentCo.Fredrick)

This statement clarifies that top management is engaged in technical rather than strategic roles to prevent the identity theft. This statement confirms Ahmad, Maynard and Park's (Ahmad, Maynard and Park, 2014, p. 366) findings that senior management was engaged in technical role to maintain the availability of technology and looks at risk superficially. This also confirms that directors or top managers are not practically involved in day-to-day fraud prevention activities.

Knowledge absorptive capacity

PaymentCo mentioned few activities whereby skills of the members are updated. They provided example using Core Personal Development (CPD) as follows:

> "*... I have to do 25 hours CPD each year... the idea is to update your skills and your knowledge base going to online with how the world changes; how the market changing in the regulations."* (PaymentCo.Pon)

This statement provides similar practices discussed by ShopingCo. Members from PaymentCo also required updating their skills annually, which is mandatory. Members also update skills by attending networking events such as conferences. Gaining more experience within the industry increases knowledge absorptive capacity. This is echoed from these comments:

> *"You get an idea what are the burning topics happening in the industry, but the long you stay in the industry, you tend to like in the first few days, and you do not understand 90% of it. After being in the industry from 5-6 years, then you understand 80 to 90 % of it, and then only 10 % of it is new."* (PaymentCo.Fredrick)

This statement confirms the element of absorbed capacity is improved by previous relevant knowledge (Cohen and Levinthal, 1990; Junni and Sarala, 2013; Jansen, Van Den Bosch and Volberda, 2005). Another interviewee also confirms this as follows:

> *"For the fraud analyst I think fraud skills are not necessarily gained in the first year. It does take several years of looking at the data, looking at the charge backs to understand where the risk is."* (PaymentCo.Jackson)

Relevant work experience helps to improve the learning experience. PaymentCo appoints experienced staff and trains them. On-job training involves working with existing colleagues to understand the nature of the work rather than attending lectures. These officials are active in absorbed knowledge.

Intra-transfer capability

Participants suggested several software used to communicate internally are summarised in (Table 5-4).

Table 5-4: PaymentCo internal communication mechanisms

Mechanism	***Use***
Video conferring	Video conferencing is used inter-branch discussion.
Email	An email is used to pass work from one team to another.
Microsoft Lync	An online chatting forum is used to discuss work and ideas.
Intranet	Centralised database

PaymentCo addressed that many teams are scattered around UK that do similar work. They also have internal colleagues located in branches within overseas. In terms of learning from members located at distant sites, they may utilise technology as follows:

> *"We have a bi-weekly team meeting where these TV hook up like a video conference. So we can see each other and have a chat, talk about merchants who are causing us problems, talking about particular trends of fraudsters of what they are doing, looking out for what transaction they are looking at high risk. Internally, yes, discussions*

> *are important. My colleague and I sit next to each other and discuss about what we can see she talk to me and then in a wider organisation LocationX [overseas] to discuss. I think that's vital to talk to her in this fieldwork."* (PaymentCo.Jackson)
> *"I normally take back the pack handed out from the events and I scan on hard drive and I send it to my team and I send them out to the team and his guys in the UK… [But I mentioning that] okay you don't need to read all of this I highlight the sections to read them I think relevant to them."* (PaymentCo.Pon)

These statements support two elements of knowledge sharing and utilisations. They share their own learning experiences, and use of what they have learnt from networking events from other organisations. They addressed the use of video conferencing for a face-to-face interaction support with internal colleagues. They use centralised knowledge base shared by risk teams only by accessing through 'intranet'. They value what they learn from peers and subsidiaries.

Motivation

They addressed natural incentive to share fraud related information with peers and the incentive is to reduce risk. Officials from PanymentCo believe that the identity theft is a general issue and collaboration in it is important. All participants supported this view:

> *"You all are essentially working towards a same goal, and you are trying to stop fraudsters and fraudulent merchants. Any exchange of detail is helpful; because the reality is that [if] the fraudsters could hit PaymentCo, [they could also hit] CompetitorCo1 and CompetitorCo2. I think there is no point of hiding information when it comes to fraud. …If you could get a fraudster prosecuted, get the police involved then it helped us. CompetitorCo1 and CompetitorCo2 helps wider source of risk and fraud community. I think really it helps to share that information and it helps latter on."* (PaymentCo.Jackson)

They were asked about their motivations to share knowledge with peers in other organisations. Similar to ShoppingCo, they could not distinguish the difference between information and knowledge. Sharing fraudsters' detail is merely sharing information. In the statement above, they have explained about their experience related to information sharing than knowledge. In the start of interview, the term knowledge was defined and explained.

Knowledge sharing structures and mechanisms

PaymentCo uses several structures to explore external knowledge as summarised in Table 5-5.

Table 5-5: PaymentCo knowledge sharing structures

Structure	***Organisation***
Forums	Merchant Risk Council
	Law enforcement conferences
	Visa and MasterCard
	European Congress
Direct – one-to-one relationships	Past colleagues
Virtual communities	LinkedIn groups and Twitter feeds

Partnership: They failed to address formation of strategic alliances similar to ShoppingCo. However, they learned new trends and techniques from subsidiaries situated overseas and utilised formal forums to explore knowledge from peers.

Official Forums: Official forums whereby networking events are organised and a good example of it is Merchant Risk Council. Officials from PaymentCo were aware about the value of networking and events. They have provided an example as follows:

> *"There is European congress turn in to get the opportunity. It is worth, because you sit there and there are hundred presentations. You have got a lot of different things. They will show you and look out through. There is a lot of list of session where people breakout into groups and have discussion about certain topics. There is a lot of presentation from different organisations about fraud and fraud trends. It is really a great conference…Visa and MasterCard do their own conferences as well."* (PaymentCo.Jackson)
>
> *So we are members of master card which is like the licence. We are not members of particular like fraud group related specifically to fraud.* (PaymentCo.Fredrick)
>
> *Its compliance e-gaming, e-money conferences whether basically advising you of update of what we perceived and what they perceived. The update is going to the regulatory framework over the course of the next year.* (PaymentCo.Pon)

On a question how they record best practices collected from these events to check their acumen and memory, one participant stated that:

> *"I might have to use something like that (Audiotape) or just take notes, because information is lost otherwise."* (PaymentCo.Jackson)

This statement shows that at the moment notebooks were used to record conference meetings. However, it can be assumed that participants were interested to use audiotape recorder, from being influenced with the recruited interview techniques from this study. A similar opinion was also found from TeleCo explained (Section, 5.4) whereby a participant addressed the use of interview to learn current trends.

Virtual communities: members who use virtual communities such as LinkedIn and Twitter expressed varieties of perspectives. Some of them also subscribe to virtual forums whereby they get weekly compliance magazine that add value to their existing knowledge. However, these members addressed lack of participation than no participation due to several reasons, such as lack of knowledge of invaluable groups, lack of time, lack of invaluable e-content shared on the groups. Unlike ShoppingCo which addressed no participation to virtual communities, informants from PayementCo addressed lack of participation.

> RQ3 (b): Why some individuals have less participation in information security knowledge sharing?

A participant commented that:

> *"I get magazine send to me every couple of weeks, specifically regarding around gambling compliance. I read those when I get chance at home and whether traveling when I have been on the plane. But in terms of active day-to-day interaction with forum participation via various pages on LinkedIn, I haven't got time to do it"* (PaymentCo.Pon)

Even though they subscribe to virtual communities, however, fail to gain proper time to participate. Therefore, they are not regular participant in networks due to time constraints. Other participant revealed no value of continuous subscription engagement in connecting with peers using virtual communities. Participant provide an example as follows:

> *"I do follow some payment professionals on twitter. I use Facebook purely for personal. I think twitter is quite useful tool for this type of industry. I do follow quite a few people on Twitter and they are purely risk and fraud based. I look at that on daily basis to find what happen to know something new on there. Somebody I follow on Twitter is talking about certain experiences and the subject then I certainly click, but I don't necessarily contact many people."* (PaymentCo.Jackson)

Some of them use virtual networks to remain updated on industry trends; however, many other participants show distrust in the information shared on virtual communities. A participant shared an opinion as follows:

> *"I use these groups to find out what other peoples are working on and what is happening, and what is relevant. I do not really use it to take information and then say to somebody that this information I have found, because I do not know how accurate it is. Sometime people's opinion [such as] someone says 30% of people that use a card spend less than £20. How I know that is accurate, just because someone wrote there."* (PaymentCo.Fredrik)

From these discussions, three elements were found that hinder the use of virtual communities as a platform for sharing knowledge. Firstly, there is time constraint. Secondly, not all groups seem to supply valuable content that support knowledge creation. Thirdly, lack of trust in the content shared through virtual communities. There is a possibility that the nature of work and time commitment may have an effect. Jacksons's background is explorative dealing with risk to look for clues that help resolving the case. Fredrick is the director of card services and Pon is the compliance manger. Nature of the responsibility varies which affect their use of virtual communities and hence their participation.

Informal social ties: Similar to ShoppingCo, officials from the PaymentCo addressed use of past ties that help to resolve issues associated with the identity theft. They utilise previous relationships. They also hide information about their customers (merchants) during the discussion and believe that sharing fraud related information is not a competitive concern. They are supportive in sharing fraud and risk related knowledge to overcome the identity theft, as follows:

> *"In a fraud and risk environment it is quite community I feel. If I phoned up an ex- colleague in PreviousCo – when you are talking about fraud you could not give away information about the merchants, but you could talk about trends and you could talk about issues. You have got sells people – they would not communicate with each other from organisations to organisation, which is understandable."* (PaymentCo.Jackson)
>
> *"It is a small industry, so you could ignore your competition. You can try to work together to find a better solution."* (PaymentCo.Fredrick)

These statements provide two views of their understanding. Firstly, they are aware of the value of their customers' information during the collaborations. Secondly, they are aware that fraud related people have a competitive advantage in sharing fraud related knowledge and trends. Therefore, PayemntCo welcomes collaboration and discussion associated with fraud related links and knowledge.

Trust and risk

PaymentCo addressed similar risk identified by the ShoppingCo, such as a leakage of valuable information during the collaboration. However, these officials could not address other risk as they normally communicate with peers on the forums. They do not have specialised strategic alliances, neither have they shown any demand to form one as evident from the following comments:

> *"I have been to law enforcement conferences. And they always run I think on Chatham house rule- where anything you say in that room will so stay in that room. Free to use information. It is say anonymised. You are happy to have a discussion about various themes. More often, you start at conference, or start at conversation or meeting and someone would say the Chatham house rule applies in there and everybody is free to discuss. Then it is not going to be open for prosecution (Laugh). It is sort of anonymous discussion. That sort of use is quite frequent."* (PaymentCo.Jackson)

Nature of knowledge

They were asked whether video conferencing is used to improve the learning experience. Regarding preference of face-to-face versus online conferencing, a participant responded that:

> *"I personally prefer face-to-face… I feel like personalised here I am watching somebody where I could easily turn off and look at my laptop and just going to my emails and he has not got a clue. Whereas actually at the events you might have the focus completely on the person who is speaking."* (PaymentCo.Pon)

5.4 TeleCo

TeleCo deals with a number of online retailers who sell gas, electricity and phone contracts online. TeleCo assists online retailers to reach their customers with minimal cost. Since the company communicates with the consumers directly and deals with personal information and financial details. Therefore, it is investigated in order to explore the measures taken to secure consumers information system. This case was motivated by an empirical investigation by Okeke (2015) where the perpetrators of the identity frauds are likely to be call centre agents. The company is profit oriented and plans to grow. However, the company could not show knowledge intensive activities. Therefore, findings from this company case study are limited in terms knowledge sharing and management elements due to its size.

5.4.1 Identity Theft Prevention Practice

TeleCo addressed two procedures to comply with customers' information security. Firstly, company implements Payment Card Industry Data Security Standard (PCI DSS). Secondly, Office of Communication (Ofcom) regulations are followed to comply with selling procedures.

TeleCo's work involves dealing with customers' information. Oliver, an outbound agent, provides an example as "*name, address, date of birth, and finally direct debit number*" (TeleCo.Oliver). Their daily work is engaged with dialler software to deal with customers' information and is stored on an internal server comes with dialler package. Considering dealing with customers' information they were asked about the security procedures. A variety of perspectives was addressed with one participant commenting that:

> "*There is definitely, obviously security management on our data. So dialler for example wouldn't save certain details. For example, account numbers, sort code, credit cards 16 digit numbers, CVV codes so these would not actually save because it is actually an import field over the script so they could actually import customer's first name, surname or address. There are no fields for them to enter any financial details. And also there is a feature on the dialler itself that pauses the call recording when taking the payment details so they can make pauses when they are taking vulnerable information they make pause in the call recording"* (TeleCo.Gizmo).

Statement from this participant suggests that a pause option may be utilised when financial details are discussed during the online sale. This stores the financial information on the server. However, TeleCo failed to address whether the agents were trained to use this option. Another participant addressed the use of an independent server which is PCI regulated to store card details supplied by customers; echoed as follows:

> "*We have recently PCI certified as a company in terms of transmission of secure data such as card details and bank details. We have to comply by PCI compliance. We have port in the back which is PCI room which is where we take card details its separate operating network. We have dialler network and all the rest of service I kept separate from PCI network there is no other information I will transfer back and forth in the same network on the PCI network we just need to take secure details such as card details and bank account details from customers*" (TeleCo.Happy).

This statement contradicts previous comments whereby the use of pause option is advised. Gizmo's statement dictates that they omit to store card details. Other interviewee raised a question in response to storing customer card details with a slight contradiction as follows:

> "*We take sort code and account numbers and we pass on secure details. What can you do with sort code account number?*" (TeleCo.Preston)

Preston believes that sort code and account number may not be applicable to defraud companies. From all specified statements, it is clear that the concern of these officials is to secure payment card, financial and banking information. Members from TeleCo are not completely aware of the value of customers' personal information and believe that fraudsters only use the card details.

5.4.2 Knowledge Sharing Practice

Knowledge absorptive capacity: To improve learning experience of members about security procedure, IT manager was asked whether any in-house training program is organised or external events are attended by members of staff and responded:

> *"We are just a small business and we need to be quite dynamic and adaptive sometimes. There will be need for any department to temporarily to come in. These guys have been here for a couple of years... We have to be flexible in terms of their skills as well they can't just focus on only one area because we are just small company and needs to be dynamic... We like to push them we don't have any structure*

> *of performance and development they all develop them for themselves"* (TeleCo.Happy)

This statement shows that there is no training offered or awareness systems are provided that guide data preservation. These members deal with customers' personal information. They need to be aware of the value of the data supplied by customers.

Intra-transfer capability: These people are situated in same geographic location under the same roof and not much efforts and mechanism are required to communicate.

Knowledge sharing structures and mechanisms

Informal social ties: Similar to previous two companies, TeleCo also addressed that peers learn new tactics and trends from employees appointed from other similar organisations. Gizmo provided states as follows:

> *"Yeah we have agents obviously who have joined our team coming from other call centres. So the agents give feedback that how the other call centres run their business or how they actually manage their side as well and they will know to a certain extent for example the dialler strategy and the data strategy they wouldn't know*." (TeleCo.Gizmo)

Gizmo shows his interest in learning from other organisations using interview technique by being influenced by interviewer. However, neither literature considered interview as strategy to gain an external knowledge, nor the other participant interviewed in this study showed any interest. Gizmo states that:

> *"The way you learn about it is really going to interviews other jobs so if you're going to interviews for the dialler management and other jobs interview from all the companies we need to get the information from the IT people exactly how you're doing right now."* (TeleCo.Gizmo)

Nature of knowledge: Nature of their work is a mixture of technical and strategic practices. Few roles addressed strategy at senior management positions such as Jessie, Happy, Preston, and Mac (Figure 4-6, Table 4-3). Outbound call centre agents possess tacit knowledge for persuading people to buy online. Others such as Nickel, Gizmo, and Oliver possessed IT skills. Most of these skills are tacit.

5.5 NetworkingCo

NetworkingCo is a none-profit organisation which provides a networking service to the online retailers. It is not an online shopping organisation as such, however due to the nature of service provided, such as networking and communication, it is considered for investigation and support findings from other organisations. NetworkingCo was investigated to confirm opinions acquired from officials. NetworkingCo provides collaboration and networking facility to communicate, therefore, is able to view the dynamics of the businesses. They have provided a clearer view on what works. NetworkingCo was investigated to comment on retailers' motivation and participation in the knowledge sharing process. This company is not large. It only recruited fewer than 100 members of staff (Table 4-2). Therefore, only two officials were interviewed from core communication position. Findings from NetworkingCo are structured as follows: Value from cross sector data is discussed. Knowledge sharing practice and extent to which subscribers of NetworkingCo are willing to share knowledge is then provided. The nature of knowledge shared is detailed. Discussing what does not provide a benefit to retailers concludes the findings from NetworkingCo.

NetworkingCo Services

The participating members who pay subscription fees founded NetworkingCo. The subscription fee depends on the size of the organisation and the value attached to knowledge exchange. The more risk appetite a company is, the more it is paying for the subscription. NetworkingCo was initially set to support organisations from the financial service sector and the underlined principle was that if the fraudsters can target one organisation, they also could target the next organisation. It was formed based on the principle that fraud is not competitive. To prevent frauds, they need to connect and collaborate. Thus, reciprocity is the key to connecting members.

5.5.1 Forum's Membership – Advantages

NetworkingCo was asked several investigative questions including the knowledge and information shared with retailers is able to reduce identity theft. Cross sector data, synthesised and domain specific knowledge found useful to help retailers in addressing and mitigating identity theft as explained below.

Cross sector data: NetworkingCo addressed two major services to help retailers in addressing and mitigating identity theft. Firstly, they share a central database consisting of the fraudsters' information amongst the subscribed retailers. Retailers use this data to check whether the person who is placing an online order is a genuine or a potential fraudster. They compare information supplied by the customer against the NetworkingCo database before shipping any goods. In response to the question whether knowledge shared through networking forums is able to reduce risk associated to identity theft, Sophie provides an answer to this as follows:

> *"We think there is value for the cross sector data that our existing members record on the database to be used in that more transactional environment. People open accounts; they try to make delivery, order goods and leave the accounts [opened]. It is very sad situation when someone opens account mostly for identity fraud related using somebody's name and current details and specify delivery address to somewhere else. So it is a case of looking at most appropriate ways to get the data into most useful part of the e-retailers chain essentially."* (NetworkingCo.Sophie)

This statement emphasises the need for effective networking forums which share knowledge among the retailers, because NetworkingCo as a communication mediator found useful medium for centralised databases. Can knowledge shared on online communities such as LinkedIn groups benefit information security professionals to reduce wheel reinvention (Tamjidyamcholo *et al.*, 2013; Feledi, Fenz and Lechner, 2013; Tamjidyamcholo *et al.*, 2014). NetworkingCo provides both online as well as offline mediums to all members to interact. This aspect has dual benefits. NetworkingCo as a communication mediator is a useful networking structure to help retailers address and mitigate identity theft. The above statement also suggests that data shared is as important as the knowledge to help address and mitigate the identity theft.

Sophie's explanation regarding identity theft is applicable to any credit granting retailer whereby customers create an online account, obtain a line of credit, place an order, and receive goods. Credit granting retailers have a great propensity to becoming victims of identity theft and related crimes. These retailers involve less financial transactions and more information. They mainly operate business on personal information supplied by their customers. Sophie agrees with this view by addressing that credit granting retailers use fraudsters' database more than other retailers do. This is view is stated as follows:

> *"We have [members from] the online retail who basically allow [customers] to set up an account ... and then they expend a line of credit to [them to] purchase again, and then customers pay off whatever [they have purchased]. So it is the less transaction, and it is the most specific area of the e-retailing sector. They will be actually looking to see we are offering a line of credit, and can this person afford it… They have many things in place which can help prevent fraud mostly around the transaction… So they are most representative of the e-retail sector. They are taking more information."* (NetworkingCo.Sophie)

This statement brings to light working operations of many retailers. There are few retailers have high risk elements associated with identity theft, whereas other may have low risk with customers' information misuse. However, it is unclear whether a centrally shared database is useful to control all types of identity theft cases, because different retailers have different risk tolerance. Sophie confirmed that a cross sector information is useful for different retailers, because it allows them to check and match fraudulent cases committed in different sectors. A suspect, who used a genuine detail to defraud a bank, can also use same detail in the retail. Thus, a shared database allows security officials to check, relate and identify identity fraud. Sophie further explains that, a risk exists when a person's delivery address does not match the current address, because there is possibility that the address on the account checks out, the name on the account checks out, the CVV (Card Verification Value) also checks out. A genuine customer may also try to defraud the retailer. This issue is already addressed in the literature review (Section 2.2). ShoppingCo and PaymentCo have also addressed this problem. Similarly, NetworkingCo have also expressed concerns about first party fraud where customers intentionally defraud companies using their own details. However, the exact value from loss is unknown due to many reasons such as; it is difficult to convince retailers that their current customers are deceiving them, and discussed first party fraud can cause reputational damage. They also find it expensive to prove that their customers are defrauding them. Consequently, companies keep it well hidden.

Synthesised knowledge: NetworkingCo updates members with synthesised best practices gained from several sources. In collaboration with s law enforcement departments such as the UK Home Office, the London Mayor's Office for Policing and Crime (MOPAC), and the National Crime Agency (NCA), NetworkingCo obtains data on how and why fraudsters steal identity information. This information is then analysed and converted into a useful report disseminated among the retailers. As such, it provides members with a fluid mix of knowledge that they can use to prevent identity theft. Ben gives an example:

> *"I have got the operational lead for NetworkingCo's engagement with law enforcement departments. The purpose of that is to try, and obtain intelligence. On how fraudsters do what they do and why. So that we can turn into something useful that members can use to prevent fraud."* (NetworkingCo.Ben)

This statement shows that the information gathered from several sources is converted into useful knowledge which is shared among members to tackle frauds. Retailers use NetworkingCo as mediator for many reasons, including its reputation to help prevent online frauds. NetworkingCo is a reputable organisation working under signed contractual governance. Sophie stated that:

> *"When an organisation joins NetworkingCo, they sign up to a set of rules. Those rules govern the use of the data. When they turn up to working party meetings, it is essentially done under Chatham House Rule. There is no formal signing on the dotted line; it is an understood principle. Mostly because the NetworkingCo's model is quite mature. The meeting themselves are being held from quite a long time. And one of those interesting things where the people who are working with fraud team change, but not necessarily the attitude of people in the fraud. So there is respect for the intelligence which is shared. Should [we] say that within the NetworkingCo meetings individual level intelligence is not shared, or someone not going to turn up and say [for example] Job Logs attend high street, or this particular solicitor or whatever."* (NetworkingCo.Sophie)

This statement addressed many valuable points. Firstly, shared knowledge is sanitised as best practice, so that retailers can trust and apply information. Secondly, they do not accept knowledge from unauthorised people. Thirdly, they have confirmed that the practice is applied and tested by an authorised member of the forum. Finally, the members trust the content shared because of the reputation of the forum.

Domain specific knowledge: NetworkingCo organises events for members to collaborate and discuss latest trends. In response to a question, whether they invite officials from a similar domain to facilitate knowledge comprehension, Sophie stated that:

> *"Everyone in NetworkingCo's membership is invited. It is basically an open invitation, obviously for sector specific. We have business sector*

> *working parties which are sector specific. This is an opportunity for people offering the same goods and services or whatever it is, who are likely to be suffering from same suite of fraud risk, to get go and to talk about fraud risk. We are not expecting someone unlikely to turn up… but [we care] how to make best use of NetworkingCo and its services. [For instance] if you turn up to organised fraud intelligence group meetings which are regionally around the country, they are cross sector. They are looking at fraud intelligence, fraud prevention specifically.* (NetworkingCo.Sophie)

The above statement indicates two kinds of conferences that help gain fraud prevention knowledge. There are sector specific and there are cross sector. Members use both to enhance knowledge. However, to discuss on an issue that retailers with better intelligence are reluctant to share their knowledge with weak ties, the participants from NetworkingCo were asked, whether some companies are better informed with the relevant knowledge than others. This question was asked to check barriers associated with power relations, and issues associated with knowledge asymmetry (Chapter 3, Section 3.4.1). ShoppingCo also found to lock-in knowledge within boundary rather than to share it with weak ties. Participants from NetworkingCo commented that:

> *"Some [retailers] are better than others. [However] again it depends on the type of product and services being offered [by them]. In some organisations, their fraud teams are fire fighting. They are not in a position to do something proactive. They are just dealing with it. Others have strategic locate on it. They are looking to make sure they are getting [a complete] intelligence from various different places. [This in turn help them] to be able to look at things given [such as] what this member had told us there, perhaps we should be tweaking some of our rules about what to prioritise and what to flag, and what sort of transaction we should be looking at, are there not so much. It is depending on risk appetite there is a range of take up of all services."*
> (NetworkingCo.Sophie)

Sophie distinguishes the nature of the reactive and proactive retailers. The organisations prone to identity theft tend to be more explorative in nature to gain strategic knowledge from various sources. The nature of work attracts members' decision whether there is value in spending efforts to gain an external knowledge. She referred to two different organisations. The first is reactive that could eliminate decisions of the members to participate in meetings. The second is proactive which gains power and strategic hold to deal cyber-attacks. This leads some organisations to perform better than others do to tackle identity theft. This supports the opinion provided by ShoppingCo. However, it also depends on the nature of the work and depends on extent to which company is risk tolerant.

5.5.2 Forum's Membership – Disadvantages

Referring back to literature review, a question was asked to evaluate what does not seem to be providing benefit with regards to the knowledge shared over forums to help address and mitigate identity theft (RQ1 (b)). NetworkingCo addressed two elements that do not seem to work. Firstly, some organisations obtain memberships to use services but avoid their own contribution. Intentionally or otherwise, some members fail to contribute their knowledge. This is expressed as follows:

> *"We have [certain] organisations who are just taking and not actually providing information…"* (NetworkingCo.Sophie)

NetworkingCo identified a number of reasons which makes participants reluctant to participate. Many retailers join NetworkingCo to access fraudulent database. Others are not interested to explore an external knowledge. Consequently, they do not value networking opportunities. Retail, banking and plastic card were found more active to contribute their knowledge, because they are the large sectors, and they have the most expensive fraud risk than the others such as fire-fighting. There are also budget constraints. NetworkingCo arranges most events in the central London. Other organisations found it difficult and costly to send their staff to attend conferences. To help improve retailers' knowledge contribution, NetworkingCo is trying to improve tactics. One of the strategies is identified as follows:

> *"We are trying to place meetings strategically to make it easy for them to turn up... [Such as] more sort of business group working party type meetings [to be organised] more regionally."* (NetworkingCo.Sophie)

In addition, the nature of retail business is quick to respond to customers' requests. They need to analyse the information supplied by customers quickly and compare fields to identify whether it is a genuine or fraudulent person. This allows them to decide quickly whether to allow customer to checkout or not. A time taking checkout process prevents customers' attention interest to shop online, and they walk away. Essentially, this is a major loss, because retailers make income from customers who buy their products. Even though NetworkingCo data is valuable to help retailers to identify an identity fraud, however, they find it difficult to process data appropriately. This is addressed as follows:

> *“The data that we hold would be of a value. [However] the challenge is to put that data in the process at the most appropriate time. [Because] the risk reward balance for an e- retailer is a bit different to other organisations that we work with. The more transaction e-retailers require data quickly to put into process. Failing to do so causes customer’s walk away. The amount of walk away from the people who fill their basket, and then find that check out process is too long. That is something that e- retailer are much more concerned with than the something possibly like a loan provider. If someone comes to you and wants to borrow 10 grand and people expect it to be a longer process than if you are purchasing the goods costing probably £100.”* (NetworkingCo.Sophie)

This statement reveals many valuable points including that there is a need for an efficient staff in the Networking organisations to process data quickly. Otherwise, retailers may find it useless, as they may lose customers. The nature of e-retailer is more sensitive to attract customers than other business organisations.

5.6 Cross-Case Comparison

Often commonly generated themes are discussed in this section. This section compares the summarised findings from different cases. Due to the nature of work, ShoppingCo and PaymentCo are more risk prone organisations to identity theft. Therefore, these organisations have a dedicated fraud prevention team. Members from these teams were investigated in depth to explore their roles and responsibilities and their knowledge sharing abilities.

Informal social ties: In all cases informants reported that there is a natural incentive to share fraudsters' information. Members also addressed the use of past ties to extract fraud prevention knowledge. Informal knowledge networks are mostly based on one-to-one relationships, however, and its use is limited to individual working in the teams. Security officials use telephone to discuss fraudulent cases. ShoppingCo and PaymentCo participants evidenced its use. Jackson from PaymentCo, for instance, recently moved from its CompetitorCo, where he was close to his past colleagues. He addressed this by sharing various contact details. This use of past ties allows both companies in a bi-directional flow of information (Almeida, Hohberger and Parada, 2011). Similarly, ShoppingCo officials trust to share security related knowledge with friends only than with other officials. They provide some examples of what they believe friends are, and whether they are trustworthy as follows:

> *"The best practices and ideas are usually shared between the friends and not at the forums, because you cannot always trust the people who can keep that information and then use it sensibly."* (ShoppingCo.Freedy)

In the above statement, it is clear that security officials are reluctant to discuss their ideas at the forums openly. Because, they are unaware who can use information wisely. Majority of the participants from a senior management favoured to share their knowledge with friends than peers. Officials from PaymentCo have also supported this and provided their opinion as follows:

> *"You tend to know people from large organisations, if they are your friends, you can give them a call to ask for ideas"* (PaymentCo.Pon)
> *"Depends what you call friends; Are they people who I would like to have a coffee with, yeah I would, but generally its work related conversation. Would I invite them to my wedding, no, they are your*

> *work colleagues first, and then they would be your friends.”* (PayemtnCo.Fredrick)

Top management sought to maintain confidentiality from competitors. Therefore, knowledge shared on current trends is only valued at official meetings organised by approved forums than informal gatherings. Knowledge on current trends is normally shared internally, regardless whether an internal peer is situated at a distance. Knowledge sharing among the peers belong to different organisations is normally what happens at organised official meetings such as conferences. Retailers consider customers' information sensitive element during the collaborations. This is evidenced as follows:

> *“Obviously, you cannot share everything about your customers. You know that our customer is the [valuable] data that we have. We should go some way to share information on fraudsters. That does happen; when we feel there is need to do that collaboration, we do that. But it is very limited.”* (ShoppingCo.Bram)

Absorptive capacity - on-job learning: Even though participants supported the notion that learning from peers is useful to improve their knowledge and efficiency to address and mitigate identity theft; most of the participants build their knowledge from on-job learning. For instance,

> “*I really think on job learning is very important. And for the fraud analyst I think fraud skills are not necessarily gained in the first year. It does take several years of looking at the data, looking at the charge backs to understand where the risk is.”* (PaymentCo.Jackson)

In the above statement, it is clear that experience improve security officials' performance and analytic ability to deal with identity theft. Therefore, PaymentCo prefers to hire experienced staff for the positions of information systems security. Even though participants were not completely denying the value from formal education, however, most of them supported learning by doing and by observing colleagues more than formal education. This is evidenced as follows:

> “*When a new starter comes in, they learn about the basics, but the important part is to sit with other fraud and risk people to learn the role, to learn the job… I think you can have all the education in the world but it is the real job training doing the analytical work that improves your analytical skills*” (PaymentCo.Jackson)

This perspective is similar discussed earlier in the social constructivist epistemology (Chapter 4, Section 4.2.2), whereby constructivist researchers believed that people make sense of their work through sharing learning experiences with others using the medium such as language and observation (Easterby-Smith, Thorpe, and Jackson, 2012, p. 23; Ringberg and Reihlen, 2008, p. 915). This is similar to the socialisation process described by Nonaka (1994, p. 19) where he asserts that businesses employ principle of on-the-job training, so that professionals can learn from each other by interacting, observing, imitating and practicing.

Intra-organisational transfer capability: Retailers are equipped with internal social media to diffuse knowledge inside the organisational boundaries. However, lack of internal trust obstructs knowledge dissemination. This aspect has been found at senior management. ShoppingCo participants have addressed intra-organisational virtual communities with the use Yammer and Shine. However, internal virtual groups are mainly formed to share company achievements rather than knowledge. PaymentCo discussed the use of company owned intranet. Findings from this study clearly show that internal virtual communities are mainly formed for spreading awareness than sharing knowledge. Companies use these communities to disseminate company and departmental achievements.

Role of knowledge manager is obvious that handle different informants and knowledge coming from many internal knowledge holders. There is need of compartmentalisations whereby access should be limited to those who are trustworthy staff and in need of updated information in the security field. Knowledge manager's role shall not only be limited to keep track of knowledge coming from various sources, but also to concentrate which members can be better in exploring, integrating and/or disseminating an external knowledge to benefit the business. Thus, knowledge can be appropriately disseminated and utilised.

Motivation: Internally security professional are motivated to teach and learn from peers. ShoppingCo and PaymentCo both have evidenced these motivations. Intrinsic motivation can be a positive factor to share knowledge with external peers. This has been tenderly utilised by Jackson from PaymentCo. However, this can bring negative impact when knowledge workers are experiencing over enthusiast to learn from peers. Unlike Tmajdyamcholo (2014, p. 29) findings which suggest that security officials negatively react to knowledge sharing when experiencing low motivation, this study in contrast have found a negative reaction when security official’s motivation is higher to get knowledge from external sources. Following quotation evidences this fear:

> *“There was a phrase that we were used to use during Second World War ‘loose lips, sink ships’. You can say too much sometimes, you can be really energetic, enthusiastic to your organisation and someone can use this against you. You have to be careful about specially security related measures, and customers, staff, supplier, and buyers’ data. Otherwise it’s very personal.”* (ShoppingCo.Freddy)

Summary of the cases: Table 5-6 shows identity theft prevention applied by the retailers. Results from NetworkingCo in Table (5-6) are considered omitted, because it provides fraud prevention knowledge than tackling with identity thieves on its own. NetworkingCo was specifically investigated to answer RQ1 to help address what is working and what does not seem to be providing benefit to the retailers in terms of shared knowledge to address and mitigate identity theft. It also commented few aspects concerning RQ2 and RQ3 to address extent to which companies are willing to share their knowledge with each other, and why some officials are less active to contribute their knowledge sharing. Therefore, Table 5-7 to 5-9 have also considered findings summarised from NetworkingCo. Findings from TeleCo are very rare due to nature of their work and size of the company was small. This company was found less intensive to knowledge management activities.

Table 5-6: Identity theft prevention measures

ShoppingCo	***PaymentCo***	***TeleCo***
Customers’ profiling	Customers’ profiling	PCI Compliance
Covert security operations	Transaction monitoring	Disabling computer ports and pen drives from staff use
Risk assessment	Credit risk assessment	
Internal deterrence policy	Internal deterrence policy	
Awareness and training	On-the-job training	
Customers’ policy	Merchants’ policy	
Compliance	Compliance	
IT-Security	IT-Security	

Table 5-7: Forum's knowledge sharing - Advantage

NetworkingCo	***ShoppingCo***	***PaymentCo***	***TeleCo***
Cross sector data	Interested in support from law enforcement	Interested in industry specific knowledge	Limited in sector specific knowledge
Synthesised knowledge	Active in gaining industry-specific and synthesised knowledge shared with senior management	Active in converting information into useful knowledge for better business decision, are able to diffuse and use knowledge within departments	Individual knowledge than synthesised shared knowledge
Domain specific knowledge	Interested mainly in the domain specific knowledge, in fraud and risk domain	Interested in domain and non-domain knowledge	Limited knowledge in information security

Table 5-8: Forums knowledge sharing - Disadvantage

NetworkingCo	***ShoppingCo***	***PaymentCo***	***TeleCo***
Lack of knowledge contribution to knowledge sharing practice by lectures	Only senior management attends organised meetings	Less contribution to share knowledge by lectures	No use of lectures to deliver knowledge
Need quick staff for data processing	Lack of knowledge manager to record knowledge	Lack of knowledge manager to record knowledge	Lack of knowledge manager to record knowledge

Table 5-9: Knowledge sharing on social media groups

NetworkingCo	***ShoppingCo***	***PaymentCo***	***TeleCo***
Nature of work is may be reactive or less prone to identity theft.	Lack of knowledge of accurate sources Lack of time Lack of knowledge grading Lack of knowledge sanitising Risk of leakage	Lack of accurate sources Lack of time	Small sized organisation – non knowledge intensive company
Imbalance knowledge level: some retailers are better in knowledge than others are.	Risk of gaining knowledge of low quality	Waste of time	Lack of resources

5.7 Summary of the findings

This study has found that companies are not willing to share knowledge on one-to-one basis unless involves in official contract. They welcome collaboration through confidentiality and data breach agreements. Trust needs to be reinforced for better collaboration. Confidentiality agreements need to be implemented. The use of police unit as a communication mediator and dedicated official forum to share retailers' knowledge is required. Information helps knowledge creation. Officials make decision based on information shared, and then turn it into useful knowledge that benefits companies. However, staff lacks to distinguish information and knowledge. Security officials found less aware of value gained from information shared at networking forums. Companies share fraudsters' information and cops contact details with each other to help detect fraud. They also share best practice in the form of security operations and other trends. They shared knowledge and information but they are not aware of it. The knowledge manager is required in this profession to manage and prioritise the knowledge coming into the organisations from different sources to benefit the business.

CHAPTER 6 DISCUSSION

6.1 Introduction

This chapter discusses findings presented in Chapter 5. The model is discussed based on answers addressed to key research questions and examines the implications. RQ1 is discussed and seeks to address what is working in the retail and what does not seem to be providing benefit with regard to knowledge sharing to address and mitigate identity theft. RQ2 addresses extent to which companies are willing to share fraud prevention knowledge with each other and under which condition(s). RQ3 evaluates why some individual either do not take part or have little active participation in information security knowledge sharing. RQ4 addressed by proposing retailers with a new extended framework to improve their knowledge sharing activities in the security profession. The chapter is summarised by discussing similarities and differences of the extended model.

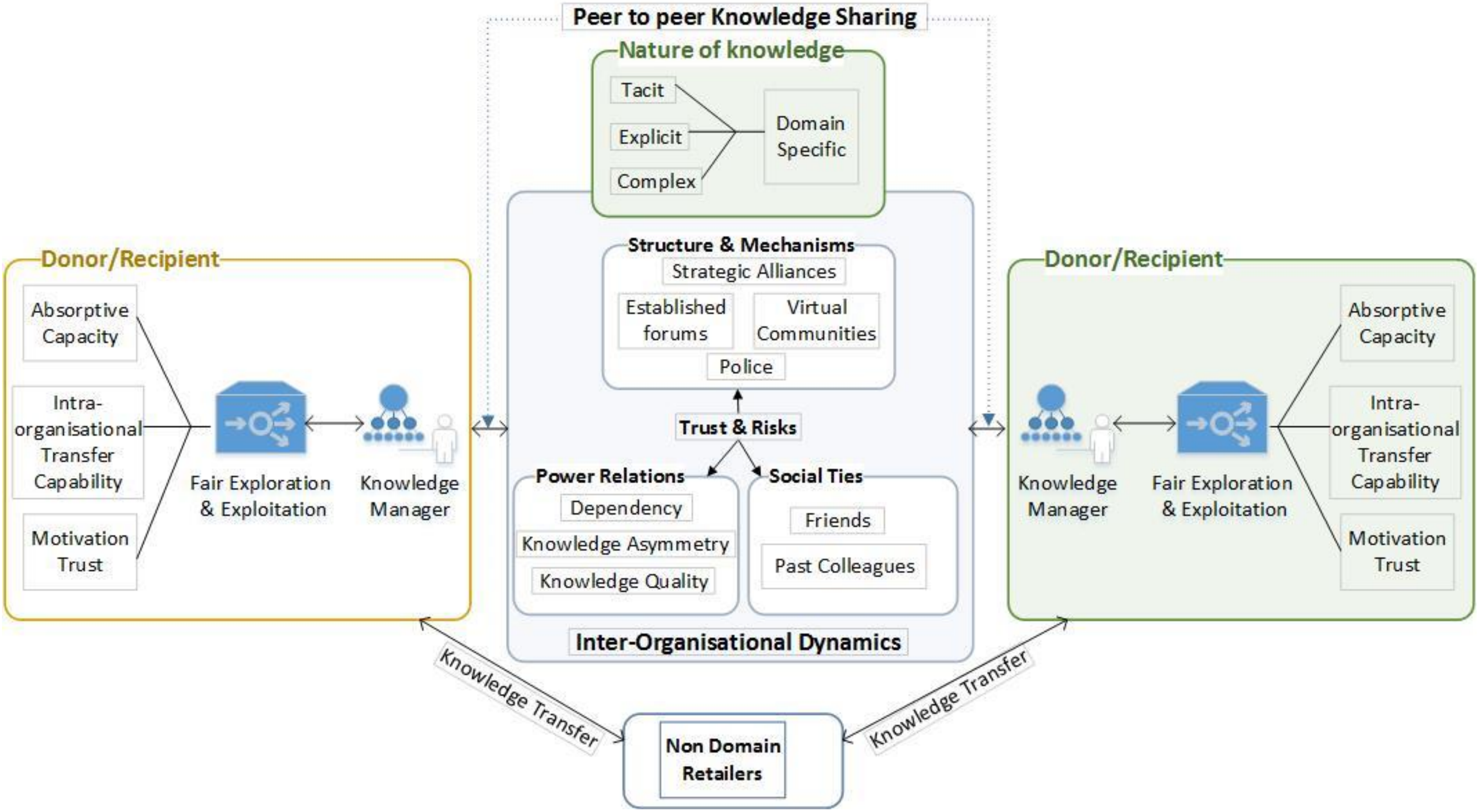


Figure 6-1: Proposed framework of inter-organisational identity theft prevention knowledge sharing in the security profession in retail

6.2 RQ1 Fraud Prevention Forums: Merits and Demerits

RQ1 (a): was asked (Section 2.6) regarding online fraud forums to explore that:

> *What is working for the retailers with regard to knowledge sharing to address and mitigate identity theft?*

The forums were useful from two perspectives: firstly, knowledge is synthesised, sanitised and then shared with members to help businesses to prevent identity theft. Secondly, the reputation of the forum gains members' trust whereby knowledge exchanged fluidly. Trusted fraud forums such as NetworkingCo, not only help in exchange of information but also assist with specialised knowledge. The information shared in these forums is converted into useful knowledge and is utilised by the security officials to benefit businesses by preventing online frauds. Synthesis of data, information and knowledge was found useful to address and mitigate identity theft. Members gain information and can convert into useful knowledge for sound business decisions. ShoppingCo and PaymentCo both agreed to this view. The risk associated with the loss of sensitive information going to competitor was not an issue when knowledge exchanged through trusted forums.

RQ1 (b) was asked to explore:

> *What does not seem to be providing benefit to the retailers with regards to knowledge sharing to address and mitigate identity theft?*

Security officials were unaware of value gained from exchange of information. On the basis of this information they make business decisions that prevents identity theft. Forums help not only to share data but also best practice. However, retailers are not fully aware of the value that can be gained from the information and knowledge obtained from forums. Retailers believe that they subscribe to fraud forums to become more aware of the burning topics about where the industry is heading.

Nevertheless, security officials who share their knowledge at the conferences also want to gain access to the police. Conference meetings are used as platform to approach law enforcement. Even though ShoppingCo shares knowledge in organised conferences to spread their reputation. Thus, are able to get police involvement in criminal investigations and prosecutions. This desire is prominent as noticed before that companies themselves cannot arrest or prevent identity thieves. Their desire to get police involvement is given as follows:

> *"Our main aim is to get into the police. Now I appreciate what you really concerned about is if we have information intelligence, we should pass that intelligence to other businesses. People guard their data and hide their data protection [strategies]... And hide behind at wrong time. Very little comes out from other end. In fact, I do not ever remember any one connected with Networking Company coming towards… So the actual I think what you are trying to get as we should all share. But I don't think when we are sharing through Networking Company that is sufficient coming from other sides. I think they [Networking Company] are trying to make changes to get it to come out but it is not at the moment."* (ShoppingCo.Jon)

This statement supports two elements: firstly, it is clear that ShoppingCo's enthusiasm to get police involvement; for them this is more important than knowledge sharing. This leads them to use networking forums to disseminate their reputation. Showing a competitive knowledge and skills assists them to create reputation. Tamjidyamcholo *et al*. (2014, p. 23) confirm this as follows:

> *"Knowledge contributors are able to gain more profit when they have the chance to show others that they have invaluable skills and capabilities."*

Secondly, this statement also shows that the retailers distrust each other. Consequently, they either lock-in knowledge within their boundaries or provides knowledge of low quality to other businesses. This aspect confirms the theory of power relations discussed in Chapter 3 (Section 3.4.1) whereby organisations either lock-in or provide knowledge of low quality to companies which lack in knowledge and other resources. A similar opinion was also extracted from NetworkingCo, with a slight contradiction:

> *"A lot of it depends on outlook of the individual organisation about whether their priority is just purely the use of data or whether they see value in the networking as well. It is not necessarily based on the size of organisations. It is more sort of the priority of organisations. It also depends on the amount of resource that is going towards their fraud teams. Some over the other if they have people they can afford to send to office to attend the meetings, because they see value in that and they do."* (NetworkingCo.Sophie)

NetworkingCo agreed that some companies are better in knowledge than others are. However, it is not their efficiency only that makes them better, but an engagement with customers' information. A credit granting company is more prone to identity theft. Therefore, they have a natural incentive to use networking events to be aware of the burning topics in the industry. It also depends on the value that individuals gain from networking. Even though ShoppingCo is a credit granting business, it does not seem to recognise full value that could be gained from networking. Participants recruited misunderstood the elements of collaboration and knowledge sharing. Consequently, they focus upon company interests than knowledge sharing.

ShoppingCo staff members were better in knowledge sharing and information exploration at networking events. However, only senior management gets the chance to attend the conferences. A participant stated that:

> *"I have been lucky because I have been at forefront of pushing managed deliveries more than Jon [Head of Intelligence] and Carl [Head of Physical Security] do, because they are not in London all the time. Being in London, I have been invited to other meetings. So I have been to new Scotland Yard a couple times at different types of meetings like intelligence sharing with their business crime hub. They are trying to open new business crime unit, which is going to [have] between 200 and 400 offices. And I met with people only a couple of days ago with regards to that so that I can show them the best practice for managed deliveries whether they are or not going to take on some of our work directly, if they do it is brilliant. ShoppingCo got legs in the door or foot in the door before anybody else."* (ShoppingCo.Greg)

From above statement, it is clear that participation to attend networking events is considered from the standpoint of geographic feasibility rather than business advantage. It was noticed in findings (Chapter 5, Section 5.6.4) that ShoppingCo does not appoint any knowledge managers who share these learning experiences with other staff, nor does this participant or other participants addressed any formal internal collaboration. Consequently, knowledge is not adequately utilised by the security officers. However, the matter of the fact is not that other members do not attend networking events. What is the benefit to explore knowledge from other organisations if it is not utilised (Easterby-Smith, Lyles and Tsang, 2008)?

A new element is therefore added to the framework (Figure 6-1) – the role of person in-charge knowledge management. This person is situated at the centre of intra-organisational and inter-organisational communication to keep track of knowledge arising from several sources so that it can be utilised effectively.

6.3 RQ2 Companies willingness to form strategic alliances

RQ2 (b) was asked to explore:

> *Under which condition(s) are companies willing to share fraud prevention knowledge with each other?*

Companies share knowledge with each other by forming strategic alliances with a desire of obtaining official contract, fair balance of knowledge sharing and human resource. Currently, there is limited interaction on official basis. Mainly individual who have strong past ties are able to gain knowledge from peers.

Online business considers customers' details vitally important during the discussions. ShoppingCo and PaymentCo believe that their customers' information going to competitors represent a major vulnerability in collaboration. During the knowledge sharing process, they may leak customers' private information. They also have addressed misuse from shared knowledge. This was explicitly addressed by fears from industry espionage, reputation damage, stealing of ideas. These are the potential barriers in initiating knowledge sharing. These results confirm the fears highlighted by Bacerra, Lunnan and Huemer (2008) who discovered that knowledge sharing is a risky and a potential vulnerable activity.

RQ2 (a) was designed to explore:

> *To what extent are companies willing to share fraud prevention knowledge with each other?*

At organisational level, companies are generally unwilling to share knowledge with each other. At individual level, officials use relationships with trusted past colleagues to exchange knowledge. The major structure for collaboration is the trusted forum. They lack to trust on a one-to-one basis except where previous bond exists with former colleagues. The prerequisite conditions that can open doors to intense collaboration is contractual governance. This is the utmost condition that may form strategic alliance between retailers. Senior management have shown desire for strategic alliances. However, their demand is trust governed (and enforced) through official contracts between the companies to exchange knowledge resources as stated:

> *"We have to trust them [first]. We do things on agreements. This is why we as business were stressing that we need a department, so that everyone's information goes in that pot."* (ShoppingCo.Jon)
> *"The forms that are signed off really release the confidentiality. Form that are signed protects the company as much as it can from misuse of information".* (ShoppingCo.Bram)

Their other condition is a fair balance of knowledge exchange from other companies. They want to collaborate with the companies to get knowledge of equal value or 'size' in return. This is evidenced as follows:

> *"…In the security world if there are many groups as ShoppingCo, more security department like ShoppingCo, it will be very easy to start having a proper collaboration. There is another company similar to ours and they have only one man who covers the whole country. He goes to talk to us (laughs). So there are more companies like ours, I think we can do it better.* (ShoppingCo.Sam)
> *"Hopefully to receive their information as well. It is Reciprocal"* (ShoppingCo.Bram)

Even though there is a strong desire to form an alliance between the companies, however, these statements suggest that organisations need to balance in the knowledge sharing and sign official contracts to regulate trust. They demand contractual governance before exchange of any information. Strategic alliance formation otherwise is of no use if they are suspicious from partner's actions or they consider themselves to hold at superior position to deal with identity thieves with regards to the knowledge and intelligence they have.

Risk of losing customers' information can be reduced by specifying off-limits (Ahmad, Bosua and Scheepers, 2014). Demonstrating to collaborating organisations how to use shared knowledge may help overcome information misuse (Yang and Maxwell, 2011). Companies addressed use of 'off-limit' by omitting name of the customers, whilst to overcome information misuse from the partners requires contractual governance (Kaplow and Shavell, 2002, p. 29).

6.4 RQ3 Online communities – Lack of participation

Section (2.5.4) had discussed that companies use virtual communities to explore external knowledge, because they are subscription free, provide access to relevant professionals across the world, there are no time or geographic constraints, and may support in a fluid mix of knowledge. In spite of these benefits, security officials were found less active to share their fraud prevention practices (Tamjidyamcholo *et al.*, 2013; 2014). To address lack of participation from exchange of knowledge on LinkedIn groups RQ3 (a) was asked to evaluate:

> Why some individuals do not take part in information security knowledge sharing?

There is substantial lack of trust in online forums. Majority of the participants at senior management position supported this opinion. ShoppingCo addressed lack of trust on virtual group to exchange security knowledge as follows:

> *"I have never seen anyone have been declined subscription [on online forums]… There are certain fraudsters and criminal organised wings siting on these forums to listen to best practices and procedures to get around it. I would, if I was a full time thief, a professional thief, I would. Wouldn't you, if that is your job and that is the way you earn your money and you feed your kids… I would go on a forum I have listened on its discussion, hide behind the PC and be totally anonymous to why I am there. So it is very big and broad forum on LinkedIn national as well as international."* (ShoppingCo.Freddy)

Freddy's statement brings many insights. First, it confirms Simpson's (2011, p. 29) statement that *"some people use the anonymity of the web to behave very badly*". From Freddy's point of view, sharing best practice using professional groups on LinkedIn would be like giving fraudsters a weapon to invade the company's network because the best practice always results from poor practice. Sharing best practice would therefore be like showing fraudsters where the company's weakest leak exists. Freddy also mentioned that there are extensive chances that leaks company's confidential information by the members from being over-enthusiastic about the online learning. Therefore, they have limited its use on workplace.

Apart from this lack of members trust on online communities, many participants also mentioned a lack of trust on online content shared. Both ShoppingCo and PaymentCo addressed this issue. A member from PaymentCo addressed this as follows:

> *"I don't really use it to take information and then say to somebody that I have found this information, because I don't know how accurate it is. Sometime people's opinion [such as] someone says 30% of people that use a card spend less than £20. How I know that is accurate, [because] someone just wrote there."* (PaymentCo.Fredrik)

RQ3 (b) explores:

> Why some individuals have less active participation in information security knowledge sharing?

Many other members working in the teams have addressed a number of concerns that make them less active to share their fraud prevention knowledge on LinkedIn groups. Majority of participants revealed lack of time to spend on online learning. ShoppingCo and PaymentCo both addressed this. Some security officials have stated that their job role is tough that they would not find proper time to learn from external peers, whereas others have questioned on the value gained from the groups. Many others have identified that knowledge provided by their own organisations is sufficient for their job role. Thus, they find no need to use efforts for external learning.

It was also mentioned implicitly that members gain subscription with groups that do not match work criterion. Sophie from NetworkingCo noted that some fraud prevention officials tend to be reactive in their work and called these "fire fighting" officials. The fire fighters may not need to learn strategic practices because all of their activity is reactive. Because of these differences of work, a suggestion is made to form groups that are sector specific. An element of domain specific knowledge is added in the extended framework (Figure 6-1) to support similar patterns of the work.

6.5 RQ4 Framework Evaluation

6.5.1 Relationship Directions

The knowledge sharing process in the extended model (Figure 6-1) is defined as a two-way relationship, whereas previous framework (Figure 3-3) identified the flow of knowledge in one direction only, from donor to the recipient. Even though ShoppingCo potentially mentioned that, they do not depend on other retailers to deal identity theft, because they are competent in tackling identity thieves. Regardless of the strength of ties, information in the knowledge-sharing environment flows to both directions. This view supports Sophie from NetworkingCo as follows:

> *"The retail, banking and plastic card are very active mostly because they are the biggest organisations, and they have probably got the most expensive fraud risk. Others are less vocal. But they all participate to some extent."* (NetworkingCo.Sophie)

Sophie in this statement confirms that all organisations participate and learn from each other's knowledge, regardless whether their nature of work is the proactive or reactive. Sophie's role is leading in the NetworkingCo and she is able to see dynamics of different organisation. Based on the findings discussed, the relationship is modified to both directions, and both firms can be donor and recipient at the same time to gain an external knowledge.

6.5.2 Inter-organisational dynamics

Trust and risk are two sides of the same coin. The riskier is the medium, the fewer retailers will trust it. The riskier the medium less knowledge would be shared. Security officials in retail trust on graded and sanitised knowledge. Therefore, they either trust organised trusted forums and police unit to use as communication mediators for knowledge exchange. Online virtual communities are distrusted for knowledge exchange. They have fears from strategic alliances from misuse of information shared. Therefore, trust and risk elements are same in the model.

Trust and risk is also connected to power relations because retailers fear from gaining knowledge of low quality from partners. They also fear from losing competitive knowledge. They have evidenced knowledge 'lock-in' to keep dependency relationship. They want other retailers to be dependant for their knowledge.

Retailers fear from leaking confidential knowledge (i.e. customers' information). Trust and risk hence is a central that either enhances or eliminates inter-organisational knowledge sharing. Previous framework (Figure 3-3) did not show relationships of trust and risk with other elements from inter-organisational dynamics.

6.5.3 Role of person in-charge – the knowledge manager

Knowledge integration: NetworkingCo clearly evidenced knowledge creation processes discussed in Chapter 2 (Section 2.3.2). Some security members collect information from various law enforcement agencies and convert it into useful knowledge to diffuse amongst members to benefit the business. Flores, Antonsen and Ekstedt (2014) call this process 'knowledge codification' which utilises company owned intranet by the knowledge worker to share their learning experiences with peers. Thus, other members can browse classified information and utilise the knowledge stored. Even though ShoppingCo is active in networking and collaboration, however, the company showed no evidence of how they convert any learning experiences gained from external events into useful knowledge to benefit the company. PaymentCo addressed this process by explaining how they turn information gained from conferences and events into useful knowledge. However, knowledge workers in this field are not fully aware whether they gain information or knowledge. For instance, informants were asked whether they gain any best practice from networking events. Following responses were addressed:

> *"It is like a day conference. So the one that I have recently attended, it was where fraud and technology collide. That was the subject of the day. Basically it was an event day where different organisations from fraud sectors get together. They are looking at what is happening in the world of fraud, how different organisations - what kind of leave as they are pulling. They are not going to any specifics but you know general trends and common themes amongst the industry."* (ShoppingCo.Debra)
>
> *"Not necessarily. No. Conferences will give you an idea to which way they think the market is going to shift towards... Now the conference that we have attended the general feeling from the industry experts is that they are so much controlled over these things, that you should start protecting this, because this is where higher risk involves in any type of currency. So on the basis of the business we have [to] set down to make decision that we are now going to start accepting this, that's only happened the last couple of weeks. So eventually decisions are made as results of the events that take place at the conferences but not necessarily best practices, because again it is something that going to*

> *rise in the same way as going to be done. There is nothing we really we can do."* (PaymentCo.Pon)

Both of these statements mentioned above, informants give a general overview of what is happening within the industry rather than gaining specific knowledge. These statements emphasised association of two important ideas. Firstly, information supports knowledge creation. Secondly, suggest that a good knowledge worker can turn an idea into knowledge (best practice); because Pon's statement mentioned that he uses ideas from the conferences to make business decisions. A dedicated knowledge manager may be needed to evaluate knowledge coming from various identity theft specialist to share with other staff working for different information security teams. This is applicable to ShoppingCo, PaymentCo, TeleCo, and NetworkingCo. Even though PaymentCo and NetworkingCo addressed this partially using a centralised knowledge base, they failed to identify a person in charge of handling these activities.

Knowledge managers should be equipped to balance knowledge exploration and exploitation. A knowledge manager may decide based on the background knowledge that which person requires to access shared knowledge and why. A manager may track knowledge coming from various sources, and keep a record of downloads to reduce internal theft. A knowledge manager can also decide whether IT-security knowledge should be accessible to compliance department and why based on nature of the knowledge and sensitivity of the matter. Based on these suggestions this thesis proposes following framework which puts knowledge manager at central position to act as a mediator between knowledge workers, management, and knowledge sharing practice.

6.5.4 Fair exploration and exploitation

ShoppingCo is active company in collaboration with external peers explore knowledge but they lack to formal internal communication to exploit knowledge within the company. PaymentCo, on the other hand is more engaged in intra-organisational knowledge transfer practice and members of the staff are encouraged to share learning experiences internally. These findings confirm Nonaka *et al.'s* (2014, p. 139) statement that separating knowledge exploration and exploitation is merely artificial. Respondents support this view. PaymentCo supported this officially by sharing staff's experiences using a centralised knowledge base (PaymentCo.Doc1. 2014). In contrast, ShoppingCo provided evidence that shows knowledge exploitation within the organisation as follows:

> *"I am in very good contact with other companies. About six months ago I shared those details with all of my colleagues via emails. I do not know if they spoke to that lady or not. No one needs to be that ahead, at least they know I was there. And in fact when I need to contact someone from other company just recently, I sent an email to my colleagues does any know this contact; and three people came back that there is the person you need to speak and there is the telephone number. So it is there but not a formal structure I suppose."* (ShoppingCo.Sam)

Internal and external knowledge structures need to be balanced to utilise knowledge adequately. Officials engaged in the practical work (i.e. identity theft analysts, advisers and risk specialists) either need to collaborate with peers or gain an access to the knowledge explored by the other members. Knowledge manager may help in this practice with fair knowledge distribution. Therefore, fair balance of knowledge exploration and exploitation is added to the firm's characteristics as an addition.

6.5.5 Domain specific knowledge

Knowledge comprehension: Section 2.3.2 discussed several theories debating on whether comprehension of tacit knowledge is achieved when shared using electronic media such as company owned intranet systems. PaymentCo's Retrieval Request Report (PaymentCo.Doc1. 2014) shows how they convert their learning experiences gained from conferences into a document that is distributed among the members of the risk department. This process confirms the theory of Nonaka's knowledge conversion. According to Nonaka's SECI model, people acquire tacit knowledge using a socialising event and convert it into explicit forms of knowledge to share with others. Participants converted their learning experiences into documents shared centrally in the repository accessed with the risk team only. Whether a shared learning experience converted into a document conveys classified information, or whether they need a face-to-face interaction afterwards, this question remains unanswered. One respondent addressed this issue directly:

> "*Since we know what we have been doing therefore there is no need of much clarification.*" (PaymentCo.Jackson)

They understand value as coming from similar patterns and trends to analyse identity theft cases. This rejects the hypothesis associated with knowledge as an objective entity that relates to the positivist epistemology whereby the world has meaning independent from the consciousness and residing in a text (Ringberg and Reihlen, 2008). Human knowledge (i.e. experience, education and intuition) is used to identify fraud patterns (Section, 3.5). The theory argued that online social web tools such as blogs are helpful in sharing tacit knowledge (Panahi, Watson and Partridge, 2013; Panahi, Watson and Partridge, 2015). Heath official use shared patterns to understand content shared on online blogs. Officials from similar domains do not face difficulty in comprehending shared knowledge (Tsoukas, 2011; Styhre, 2004).

Positivists believe that the richness of the communication mechanism can overcome barrier with knowledge comprehension (Chapter 4, Section 4.2.1) similar to Panahi, Watson and Partridge (2013; 2015). They support the idea that social networking sites can overcome hurdles associated with understanding of tacit knowledge shared over electronic medium. Social web tools such as blogs and other social networking sites can overcome some of the barriers associated with the articulation and understanding of knowledge that is embedded in the mind of a knower.

It is not the richness of communication mechanism only that supports this comprehension but the use of analytical abilities of the mind to identify similar patterns. Chapter 2 (Section 2.3.2) proposed that the domain specific knowledge holders might not lose value completely by converting tacit knowledge into explicit. Knowledge comprehension has strong relationships with the knowledge absorptive capacity whereby prior related knowledge supports knowledge articulation and improved understanding. Prior related knowledge enhances knowledge absorptive capacity is supported (Cohen and Levinthal, 1990). Moreover, these teams are doing similar jobs, there is a little effort required to convey the message. Even though similar patterns of work help knowledge holders to relate security procedures, however, the majority of participants from all companies support face-to-face interaction for a complete understanding of what their peers do.

6.5.6 Police-retailer relationships

Two divergent and often-conflicting discourses emerged from ShoppingCo and NetworkingCo. Firstly, a group of participants suggest that making collaborative relationships with police force is useful to obtain police support in business crimes. Thus, ShoppingCo appointed field-based investigators from a policing background. They also create a close collaboration with police forces in their region. Similar opinion is also extracted from NetworkingCo whereby Ben discuss about retailers and police relationships as follows:

> *"Most of them have their own dial up relationships with police forces. Up until about 2 or 3 years ago the "action fraud" reporting mechanism was not as rolled out as it is now. So businesses particularly retailers would have to found their own relationships with local forces in order to do that sort of operations."* (NetworkingCo.Ben)

Secondly, they report frustration from the police force and states that past ties do not work, as efficiently when they were member of the official forces. They stated that the police response with business crimes is not optimal, echoed as follows:

> *"Now it is quite interesting last year we supplied 25,000 frauds that were perpetrated on ShoppingCo... Sadly out of that only 11 came to some fruition with the Police. So that is how bad it is. Although we reported it does not get dealt with."* (ShoppingCo.Greg)
>
> *"Police have not got an appetite to investigate a fraud at our level... they have not got the willingness just to be honest."* (ShoppingCo.Sam)
>
> *"Usually the police force does not actually have enough experience in this dedicated field to understand complexity of the offence."* (ShoppingCo.Freddy)

The participants educated police with the understanding of business crimes through lectures and talks. There is a gap as to address why retailers lack to get police support? Other informants stated reason that address these gaps as echoed:

> *"First, limited resource or other priorities [by the police force are different]"* (ShoppingCo.Opt2)
>
> *"These cases scored and action based on prioritisation within their system"* (NetworkingCo.Sophie)
>
> *"If you ask most police officers why they have joined the police, most of them can say to deal with fraud, to arrest a murderer and to arrest the burglar. And police priority up until the last and least, probably up until from the last 10 years has all been focused on things like drug, robbery and the violence crime that actually harm individuals. Whereas*

> *financial crimes are basically more than theft and that is not really a glamorous sort of work police get involved with."* (NetworkingCo.Ben)

A number of factors cause lack of contribution from the security professionals. Firstly, the police lack expertise in business crimes. Secondly, insufficient resources and lack of funding hinder police support in mitigating identity theft. Thirdly, the nature of work is different. Dealing with identity crimes is not as fascinating as dealing with murder cases. There is a view from other participant who identifies lack of proper utilisation of police resources in business crimes. A participant was asked to share his experience of powerlessness whilst comparing his time with the police:

> *"It is massively frustrating. Because I cannot use any of the intelligence tools that I used to be over there to tap into when I was a police officer... I was used to go to the police national computer and used to check on the registration marks to the cars. Now all I can do is to pass it through action fraud... Again the bigger picture than that bit of intelligence can be added into that job wherever it might be."* (ShoppignCo.Greg)

Thus, there is a clear need for a unit that supports business crimes and the exchange of knowledge. Relationship building or producing legal evidences of high quality by the retailers alone is not working optimally.

6.6 Summary of the chapter

This chapter has discussed various research questions based on the findings elaborated in Chapter 5 as background knowledge. The extended framework is discussed and new emerging themes are elaborated. The next chapter highlights contribution of the study, implications and recommendations by reviewing research aims and objectives and major findings.

CHAPTER 7 CONCLUSIONS

This chapter revisits the research aim, objectives, and key research questions to specify major contributions of the study. Key findings are addressed and implications are discussed. Challenges and the limitations of the study are identified to specify future promising research areas. Recommendations are drawn. The chapter concludes with reflection.

7.1 Research objectives

Various existing identity fraud prevention practices were evaluated and discussed in Chapter 2 (Section 2.2.3) to help address research objective 1 (OBJ1). In addition, however, new practices were also investigated within ShoppingCo, PaymentCo, TeleCo and NetworkingCo that attempt to prevent identity theft. These practices are summarised in a new model (Figure 5-1). This new model highlights a scheme that a large retailer employs to prevent identity theft. This scheme may help retailers to design or redesign their security practices, because it provides a clearer understanding of innovative practices implemented by the retail industry. This new model contributes to objective (OBJ1). However, this model does not address retail-to-retail collaboration and knowledge sharing. This aspect is considered in research objective (OBJ3).

Chapter 2 (Section 2.3 – 2.7) and Chapter 3 have discussed existing knowledge sharing within companies across a broad spectrum of business presented in the literature to address research objective (OBJ2). Retailers' existing communication elements were addressed and knowledge sharing practices were discussed. Current formal and informal communication practices were also synthesised. This synthesis suggested that information security officials were less active to contribute fraud prevention knowledge with external peers (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Liu, Ji and Mookerjee, 2011; Tamjidyamcholo *et al.*, 2014). The need for a comprehensive framework that considers all aspects of inter-organisational knowledge sharing in the security profession was addressed. Three frameworks from recent literature were compared and contrasted (Yang and Maxwell, 2011; Bigdeli, Kamal and Cesare, 2013) to identify a suitable framework to evaluate knowledge sharing practice in the security profession. A framework of the factors influencing inter-organisational knowledge transfer (Figure 3-3) was chosen to evaluate how identity theft prevention officials share fraud prevention knowledge (Easterby-Smith, Lyles and Tsang, 2008).

Evaluated frameworks raised many concern including whether domain specific knowledge is able to prevent identity theft; whether retailers are able to understand practices used by their peers; whether online fraud forums are able to provide invaluable information that attempts to prevents identity theft; whether is there any benefit to exchange knowledge with non-domain retailers that help prevent identity theft?

This study chosen ShoppingCo, PaymentCo, TeleCo and NetworkingCo to answer these issues. This criterion assisted in addressing OBJ3 designed to select a suitable business to investigate the topic. These companies were found susceptible to identity theft related crimes, because they operate business online. These companies have high-risk elements, because they grant online shopper with a credit to buy their products. Credit granting online retailers were found subject to identity theft and related crimes. Criteria were set out to consider companies which provide rigorous understanding and knowledge based on these businesses to tackle identity theft.

Findings evaluated from ShoppingCo, PaymentCo, TeleCo and NetworkingCo helped to extend the framework applied within the information security in retail to prevent identity theft. This study assessed how different retailers share identity fraud prevention knowledge with each other by investigating knowledge sharing practices (OBJ4). As a result of this evaluation, an extended model (Figure 6-1) is discussed and proposed to improve knowledge-sharing practice within the security profession. The extension of the framework helped to address research objective (OBJ5). These objectives are mapped in Table 7-1. Key research questions with key findings are also addressed (Table 7-2).

Table 7-1: Mapping study research objectives into Chapters

OBJ	***Research Objectives***	***Chapters***
1.	*To investigate various identity theft prevention practices by reviewing the literature and published reports.*	*2, 5*
2.	*To investigate existing knowledge sharing within companies across a broad spectrum of business presented in the open literature*	2 and 3
3.	*To select a suitable business to investigate based on the knowledge and understanding obtained from rigorous literature review and analysis.*	1 and 4
4.	*To assess how different organisations share identity fraud prevention knowledge with each other by investigating knowledge sharing practices within three organisations in the retail industry and with a networking forum.*	5
5.	*To propose an extended knowledge-sharing framework within the security profession.*	6

7.2 Research questions

Table 7-2: Research questions and important findings

RQ	***Research Question***	***Important findings***
1.	*What is working for the retailers and what does not seem to be providing benefits with regard to knowledge sharing to address and mitigate identity theft?*	Forums, contractual governance, security conferences and events support both information and knowledge sharing to address and mitigate identity theft
2.	*To what extend are companies willing to share fraud prevention knowledge with each other and under which conditions?*	Alliances formation is demanded by participants with contractual governance to open doors for closer collaboration
3.	*Why some individuals either do not take part, or have less active participation in the information security knowledge sharing?*	Lack of time, lack of fair knowledge about relevant online forums, lack of trust on online knowledge
4.	*Which is the best knowledge-sharing framework in the security profession in retail to facilitate an understanding of inter-organisational knowledge sharing practice?*	Figure 6-1 has devised the component to persuade knowledge worker in the security profession

7.3 Contributions

The novel contributions of this study are: Firstly, this study adapts a conceptual model and evaluates its various components to seek how security professionals hired in online retail, share their learning experiences. As a result of this the evaluation, the applied model is extended, and recommendations are drawn. Secondly, a new model is devised based on how security officials in the UK retail deal with identity thieves. Role of various stakeholders and their collaboration to prevent identity theft is discussed. Thirdly, this study contributes to methodological implications identified in the knowledge management literature. Previous studies had stated that surveys are not effective enough to explore richness of knowledge sharing practice in the security profession. Finally, the concept of identity theft is clearer. Identity fraud risk with various online retailers are distinguished and discussed. This contributes to an improved understanding of the identity theft prevention practice. These contributions are discussed in detail as below.

7.3.1 Extended Framework of Factors Influencing Inter-Organisational Knowledge Sharing

This thesis contributes to addressing the knowledge gap identified by previous studies involving an urgent need to explore lack of participation from security officials to knowledge contribution to the knowledge sharing practice (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Tamjidyamcholo *et al.*, 2014). This study has taken into account a holistic perspective of inter-organisational knowledge sharing practice in the security profession. Some studies considered partnership (Flores, Antonsen and Ekstedt, 2014; Liu, Ji and Mookerjee, 2011), while others concentrated on online web such as social media groups (Tamjidyamcholo *et al.*, 2013; Feledi, Fenz and Lechner, 2013; Tamjidyamcholo *et al.*, 2014) to investigate how information security knowledge is shared among peers. Findings from this study extend knowledge gap discussed by Tamjidyamcholo *et al* (2014, p. 31). These authors have covered global virtual communities and have found that local virtual communities such as inter-organisational and internal groups used by security officials have yet to be explored with respect to its use in the information security knowledge sharing. In addition, official forums that provide security knowledge were of less interest to the researchers with regards to address and mitigate identity theft. Offline forums and virtual communities were explored superficially in this field of study. Many factors that provide insights on what is working and what does not seem to provide benefit to the retailers were explored. This research has combined various aspects into a single comprehensive study.

This study extends a framework of inter-organisational knowledge sharing in the security profession, to help security officials with improved knowledge and learning experience. A model to discuss peer-to-peer communication and knowledge sharing practices has been applied (Figure 3-3) and extended into a new model (Figure 6-1) as a novel contribution to the security profession. This study has applied a generic framework of factors influencing inter-organisational knowledge transfer (Easterby-Smith, Lyles and Tsang, 2008) to investigate peer-to-peer collaborations in online retail. In particular, the framework is applied to explore how identity theft prevention specialists hired to secure business information systems communicate with each other to share fraud prevention knowledge. This study, however, does not limit an evaluation with pre-identified themes only. The design of semi-structured interview allowed the exploration of new patterns repeated by several participants. Documents explored from the security officials suggested the identification of new themes essential for knowledge sharing and collaboration in the security profession. This evaluation helped to address a number of new elements to enhance collaboration among security officials. As a result, new model is devised as an extension to accommodate these new themes that influence inter-organisational knowledge sharing. The extension of this new model is discussed as below.

Most of the elements in the extended model remain the same. This new model assumes both organisations as donor and recipient at the same time. This is a new addition which shows knowledge flow to both directions. Characteristics of both firms such as knowledge absorptive capacity, intra-organisational knowledge transfer capability and motivation to teach and learn are the same. A major contribution of the extended model is the specification of a role of the manager as facilitator or “gatekeeper”. This is a major characteristic of both firms in the model. For this knowledge manager’s role, two kinds of personnel seem more effective. Firstly, a communication specialist acts as a hub between the management and the employees. This person may be able to coordinate and manage the knowledge sharing process effectively due to the background experience of dealing with internal and external sources. This person, however, may or may not be bale to evaluate the content shared from the security background. Secondly, an official from a police background would suit this position. This new role may also require a relevant background in the information security domain, such as an official from a police background. This suggestion is based on the evaluation of background knowledge gained from participants. Most of the participants were retired police officers. They were successful in detecting suspects and were able to obtain police collaboration in the fraud cases to prosecute identity thieves. These officials also seem active in opening doors for further collaboration. This may help to bridge the gap found between police and retailers communications (Chapter 6, Section 6.5.6).

This extended model has also identified an imbalance in the practices of knowledge exploration and exploitation. A major barrier to knowledge utilisation found was the lack of formal knowledge dissemination within the teams. Chapter 5 has highlighted that only a few officials from senior management gain an opportunity to exchange knowledge with external peers. Actual knowledge workers such as analysts, identity theft specialists, and IT-security personnel failed to share knowledge with external peers through formal collaboration. Some retailers (i.e. ShoppingCo and NetworkingCo) were better in exploring knowledge from external peers. Others (i.e. PaymentCo) were advanced in the knowledge dissemination within the firm. PaymentCo evidenced the use of intranet knowledge base and use of videoconferencing to exploit internal knowledge. ShoppingCo failed to show internal knowledge dissemination as a formal practice. Knowledge manager as a facilitator may be is able to identify the person who is able to explore relevant knowledge from external peers more effectively. This person in charge may also be able to find out the person more effective to integrate new knowledge within the existing body of knowledge base. Knowledge manager may be is able to make proper decisions based on this background knowledge to overcome barriers associated with knowledge utilisation. These decisions may help to reduce the gap between improper knowledge exploration and exploitation.

In the centre of the extended model (Figure 6-1), interactive dynamics between the firms show the factors such as structures and mechanisms, power relations, trust and risk, and social ties. To discuss inter-organisational dynamics between the organisations, Easterby-Smith, Lyles and Tsang (2008) have identified two major structures such as networks and strategic alliances to share knowledge among the knowledge workers. The extended model also discussed role of police units, established forums and virtual communities to share fraud prevention knowledge. These new elements are added in the extended framework as a novel contribution. Previous studies in the information security domain show that virtual communities such as LinkedIn groups failed to communicate fraud prevention knowledge due to lack of interest from the security officials (Tamjidyamcholo *et al.*, 2013; Feledi, Fenz and Lechner, 2013; Tamjidyamcholo *et al.*, 2014). One such lack of interest was lack of sanitised knowledge shared on the online groups. Security professionals prefer to either use police units to exchange knowledge resources or use online trusted forums. These new elements are added in the extended framework. Some officials also use informal social ties generated with past colleagues and friends to explore external knowledge; this behaviour confirms construct from the applied framework (Figure 3-3).

Communication with non-domain retailers to gain an external knowledge was also lacking from previous model. This study has found that retailers also use non-domain peers to gain an external knowledge that help prevent identity theft. Therefore, communication with non-domain retailers is added in the framework as an additional element at the bottom of the diagram (Figure 6-1).

7.3.2 New Framework of Factors to Prevent Identity Theft

A new framework (Figure 5-1) represents comprehensive communication between various stakeholders at national and international levels. This new framework is intensively structured, which considers current security operations and protocols. Previous studies, however, only focused on organisational factors such as policy, deterrence, IT-security and risk assessment. This new model, in addition, also incorporated external factors as a novel contribution to address and mitigate identity theft. These external factors discussed the role of the agencies including, law enforcement, retailers, courier companies, and outsourcing firms. Security managers and policy makers will find it useful.

7.3.3 Contextual details

Methodological implications mentioned in the previous studies were addressed with the use of qualitative studies. Previous studies have found that use of surveys may not be effective to explore depth of the knowledge sharing practice in the security profession (Flores, Antonsen and Ekstedt, 2014; Tamjidyamcholo *et al.*, 2013; Tamjidyamcholo *et al.*, 2014). Contextual details are intensively studied using qualitative cases. Previous studies to evaluate fraud prevention knowledge were mostly conducted using survey. This study considered an intensive evaluation of various cases. Real insights were gained by conducting face-to-face interviews. There were organised discussions with security officials, and informal meetings such as a discussion over a cup of coffee to discuss current security measures were also tape-recorded.

7.4 Implications and Recommendations

Practices and policies about knowledge sharing in the online retail environment may vary from region to region, country to country, company to company and unit to unit (Styhre, 2011; Szulanski, 1996; Easterby-Smith, Lyles and Tsang, 2008). In the UK only, these findings can be applicable to the retailers which grant credit to the customers to buy products from them. Retailers more prone to identity theft may benefit from the conclusion drawn. However, some of the aspects of the study can be applicable worldwide. For instance, knowledge absorptive capacity requires every knowledge worker to understand patterns of another peer's knowledge.

7.4.1 Knowledge Manager

An important suggestion of this study is the role of a person in charge of knowledge management initiatives. In previous sections, two kinds of people were suggested to take position of the knowledge manager in the security profession. Firstly, communication and facilitation specialists would be able to create more links for external collaboration. Secondly, an official from a police background would be naturally trained to deal with the suspects. An official from a police background is more skilled in the confidentiality and security related matters. Thus, sensitive data may not be exposed to the external peers. Either business lock the information which is sensitive, or they expose to the risk of unauthorised entries (Ahmad, Bosua and Scheepers, 2014). They either may consider the process of facilitation in the collaboration or the confidentiality and security.

This study recommends retailers to hire a person from a police background or give this position to an existing member hired from past police background such as former police officers. This may enhance knowledge management activities. A knowledge manager from a police background would be helpful in security related activities to investigate fraud cases and would be able to help prosecute the suspect. An additional benefit would be to manage knowledge resources. Security professionals need a person in charge to transform and integrate knowledge to be utilised adequately. There is need for a role to keep track of security professionals' knowledge and knowledge management activities. Except NetworkingCo, none of the other companies addressed a person in charge who manages knowledge coming from different sources. PaymentCo addressed the mechanism through a centralized database. However, they failed to provide staff to keep records of security officials' knowledge. NetworkingCo addressed a person in charge. The participant Ben keeps track of the information coming from law enforcement departments. However, NetworkingCo did not provide a dedicated member of staff to keep records of security officials' knowledge shared at these events.

There is also a barrier between the collaboration of information security staff working with the computers (such as identity theft prevention advisers, analysts, IT security personnel) and on-the-ground investigators, tracking the potential fraudsters. There is also a third link of official authorities such as police. The police arrest the suspect Chapter 5 (Section 5.2.1). There is lack of coordination among these three stakeholders. Their collaboration is essential to help identify and arrest an identity thief. However, there is gap between police and retailers collaboration discussed in Chapter 6 (Section 6.5.6). These various boundaries have to be bridged. The first two groups such as security officials and on-the-ground investigators work within the company. A knowledge manager for efficient knowledge exploration and exploitation can coordinate these stakeholders. However, the third link between the company and official authority requires closer collaboration to deal with identity crimes. The official authorities allocate resources to deal with black-collar criminals such as murderers, money-launder, traffickers and terrorists, whereas retailers want to arrest and prosecute white-collar criminals to recover the amount lost. The police are allocating more resources in combating Internet crimes. The retailers are also allocating resources to deal with the cyber criminals. This shows that their interests are converging. They are coming closer eventually. Retailers have initiated closer collaboration through running training programs to show police how to deal with cyber criminals. Police is lacking in this area, since their expertise and interest are more equipped to deal with murderer and other black collar criminals. There is need for effective cooperation and trust between the police and the retailer. The companies are determined to source police collaboration. As a result, a knowledge manager from a police background may enhance police-retailers coordination. Officials hired from police background may be better equipped to deal with the business crimes, because of their wealth of the knowledge to deal the suspects.

The officials from police background may retire with an autocratic behaviour, because their job nature is strict. As a result, this person may not be better equipped for the knowledge management activities. A person with an autocratic behaviour may fail to deal with different knowledge workers. Therefore, requires strategic training programs to guide their attitude. Greg from ShoppingCo is a person who attends external meetings. He specified that he trained on several courses in the security and confidentiality during his services as a police officer. For instance:

> *"I have not been on management courses to manage people or anything else. All I have is a 30 years of experience. I can give evidence on counterfeit American currency. I am expert in the ATM fraud, which is based on my experience as a Police Officer. I have taken surveillance courses. I have taken detective training courses on how to handle informants. All of those national trend courses through the police, I can bring to the table in this job. So I don't train people like to be surveillance officer or handle informants but I'll give them advice generally."* (ShoppingCo.Greg)

This statement above implicitly suggests that business might consider to organise management training courses for knowledge manager hired from a police background to train them how to manage people and the knowledge. They may thus learn an attitude of facilitation and collaboration as a resource person. To overcome an autocratic behaviour, business may require management courses for these officials.

Managing that relationship is probably easier than managing the security. This study, therefore, suggests the use of former police officers in the model than communication specialist to impart the role of knowledge managers, because security is ultimately more important than knowledge sharing. In fact, the process of knowledge sharing is advised to improve the security measures. Knowledge sharing facilitates security operations. To secure information systems more effectively requires more knowledge sharing.

7.4.2 Trusts and Risk

Trust is a general issue and applicable to online groups of any nature. However, these findings are appropriate in the security professionals, because their work involve fraud, risk, analysis and the investigations. By nature, security officials who seek to prevent identity fraud are suspicious. The respondents in this study mainly were fraud detectives which require customers' valuable data for their normal day-to-day activities. Thus, their knowledge was highly sensitive commercially leading to operational staff being reluctant to communicate openly with external peers. The components amended in the framework (Figure 6-1) may help retailers to improve knowledge management initiatives. However, trust is applicable in the domain of information security as this discusses use of contractual governance.

The recommendations provided may help retailers to consider factors effecting collaboration between security professionals leading to improved trust. This work may help decision makers and managers in designing and implementing security procedures for the important data. They can also consider the redesign of their fraud prevention departments based on suggestions proposed by this study. Compartmentalisation can overcome risk of losing important knowledge. Limiting information flow and specifying off-limit knowledge can significantly reduce the degree of risk involved with the loss of important and confidential information such as customers' invaluable details and competitive knowledge (Ahmad, Bosua and Scheepers, 2014). Contractual governance among the organisations may improve the trust among them and information misuse can be controlled. Retailers are reluctant to communicate with peers who possess weak ability to tackle identity theft. Unsettled policies and practices often lead to creative solutions (Sammarra and Biggiero, 2008). They may be helpful in invaluable knowledge.

7.5 Challenges and Limitations

A number of limitations need to be addressed. Most notable are the methodological limitations. There is a need to either improve methods of approaching security officials or enable this type of work to be conducted through university, business and law enforcement collaborations. Failure in this regard causes limited access to potential participants.

There is a gap between the data collected from ShoppingCo and other companies. The study plan considered 10 to 12 interviews to facilitate cross case comparisons. The information security field involves financial information incorporating customers' personal details and this data makes the investigation sensitive. Convincing the participants to obtain accurate facts was challenging. Most participants were reluctant to give details regarding their roles and responsibilities. Senior managers in ShoppingCo provided access to more participants. A meeting was scheduled because of this access with the Fraud Department at a different site. Even then, the participants were not ready to initiate discussion unless they confirm from headquarters. This caution is summarised by following quotations:

> *"I can't tell you, it is so confidential."* (ShoppingCo.Freddy).
> *"Apology I was a bit vague, because I had not been actually given a background or any detail. As you can appreciate the sensitivity we do as department. But that's fine. Do what you need to do."* (ShoppingCo.Debra)

This issue was also experienced during data collection in the TeleCo. Preston from TeleCo was approached through the snowballing technique, whereby his colleague provided his contact details. He was approached on the telephone and agreed for a face-to-face meeting. Even then, before giving any detail he raised a number of probing questions such as:

> *"Who is your main source of contact in our company? How did you come to know about us?"* (TeleCo, Preston)

ShoppingCo referred access to ShoppingCo2. Initially, they agreed to provide access to at least 10 interviews but later changed their mind. As a result, only one interview with the Head of Security was possible.

7.6 Future Work

This study has highlighted several factors that make security officers reluctant to use official forums. Insights from security officials are addressed that hurdle their participation to contribute their fraud prevention knowledge. Future studies may investigate how to engage better online forums to maximise effectiveness of the knowledge sharing practice based on these insights. Further research can be conducted in public sector and inter-agency (law enforcement) collaboration and is outside the scope of this study. However, collaboration with public-private sector is a promising future area where the role of government agencies such as law enforcement, fraud bureau and police collaboration can be explored further. Evaluating the sectors in other contexts such as Germany, France, USA, Canada and Australia can extend these findings.

The future researcher may overcome the barrier with data collection by open-ended survey to explore both quantitative analysis and views from participants. This methodology may help future researchers to overcome the limitation associated with access to limited number of participants.

7.7 Reflections

The participants recruited were of different ethnicities but with a British background. The author of this thesis belongs to a different national culture. Understanding and familiarity with local culture is essential to understand the subtle nuance between people. In this regard, postgraduate certificate in business and management research methods was obtained during at MPhil stage of the thesis. This certificate assisted in understanding and overcoming cultural barriers. Interview protocol was piloted prior to the main study data collection. British born investigators might have taken for granted various common themes. As an outsider, the authors of this thesis, had an advantage to notice and question wherever an insider might have had made assumption.

Research program was approved in May 2013. Research ethics approval was obtained in April 2014 before field investigations. MPhil stage to PhD was transferred in July 2014. Thesis was written up and submitted in June 2016. The title of the thesis, the research aims and objectives however remained the same. There was slight change in the research questions based on preliminary understanding and the field visits. Question were further refined after field visits (Miles, Huberman and Saldana, 2014; Yin, 2009). Feedback on research paper from Editors of journal of Computers and Security was utilised to refine the key research questions.

Each previous step from the stages was made simple by a move to the next. Each subsequent stage ahead was found to be increasing challenging. However, research process developed the understanding, experience and expertise and to improved knowledge in the field.

REFERENCES

Aerohive Networks (2013). *The Benefits of Cloud Networking- Enable cloud networking to lower IT costs and Boost IT productivity,* Sunnyvale CA, Aerohive Networks, Inc.

Ahmad, A., Bosua, R. and Scheepers, R. (2014). 'Protecting organizational competitive advantage: A knowledge leakage perspective'. *Computers & Security,* **42** (2014), pp. 27-39.

Ahmad, A., Maynard, S. B. and Park, S. (2014). 'Information security strategies: towards an organizational multi-strategy perspective'. *Journal of Intelligent Manufacturing,* **25** (2), pp. 357-370.

Ahuja, G. and Novelli, E. (2011). 'Knowledge Structures and Innovation: Useful Abstractions and Unanswered Questions'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organizational Learning and Knowledge Management*, pp. 551-578. Chichester, UK, Wiley Online Library.

Alavi, M. and Denford, J. S. (2011). 'Knowledge management: Process, practice, and web 2.0'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organizational Learning and Knowledge Management*, pp. 105-124. Chichester, UK, Wiley Online Library.

Alavi, M. and Leidner, D. E. (2001). 'Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues'. *MIS quarterly,* **25** (1), pp. 107-136.

Albrechtsen, E. and Hovden, J. (2010). 'Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study'. *Computers & Security,* **29** (4), pp. 432-445.

Algeier, C. S. (2015). Response to the request for comment noted in the March 4, 2015 Federal Register notice announcing the public ISAO/ISAC Summit on March 18th to M. A. Echols. 17 April 2014.

Almeida, P., Hohberger, J. and Parada, P. (2011). 'Informal knowledge and innovation'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organizational Learning and Knowledge Management*, pp. 383-402. Chichester, UK, Wiley Online Library.

Andersen, P. H., Kragh, H. and Lettl, C. (2013). 'Spanning organizational boundaries to manage creative processes: The case of the LEGO Group'. *Industrial Marketing Management,* **42** (1), pp. 125-134.

Argenti, P. (2013). *Corporate communication,* New York, United States, McGraw-Hill Higher Education.

Arturo Lowensberg, D. (2010). 'A “new” view on “traditional” strategic alliances' formation paradigms'. *Management Decision,* **48** (7), pp. 1090-1102.

Awad, E. M. and Ghaziri, H. M. (2007). *Knowledge management*, Delhi, India, Dorling Kindersley Pvt. Ltd.

Barney, J. (1991). 'Firm resources and sustained competitive advantage'. *Journal of management,* **17** (1), pp. 99-120.

Barney, J. B. (2000). 'Firm resources and sustained competitive advantage'. *Advances in Strategic Management,* **17** (1), pp. 203-227.

Barney, J. B. and Hesterly, W. S. (2015). *Strategic management and competitive advantage: Concepts,* Boston, Pearson.

Barringer, B. R. and Harrison, J. S. (2000). 'Walking a tightrope: Creating value through interorganizational relationships'. *Journal of Management,* **26** (3), pp. 367-403.

Bashir, M. S. and Khan, M. N. A. (2015). 'A triage framework for digital forensics'. *Computer Fraud & Security,* **2015** (3), pp. 8-18.

Basit, T. (2003). 'Manual or electronic? The role of coding in qualitative data analysis'. *Educational research,* **45** (2), pp. 143-154.

Becerra, M., Lunnan, R. and Huemer, L. (2008). 'Trustworthiness, Risk, and the Transfer of Tacit and Explicit Knowledge between Alliance Partners'. *Journal of Management Studies,* **45** (4), pp. 691-713.

Bhattacharyya, S., Jha, S., Tharakunnel, K. and Westland, J. C. (2011). 'Data mining for credit card fraud: A comparative study'. *Decision Support Systems,* **50** (3), pp. 602-613.

Bigdeli, A. Z., Kamal, M. and Cesare, S. d. (2013). 'Information sharing through inter-organisational systems in local government'. *Transforming Government: People, Process and Policy,* **7** (2), pp. 148-176.

Bindra, G. S., Shrivastava, D. and Seth, R. (2012). 'With attackers wearing many hats, prevent your "Identity Theft"'. *In Proceedings of the 6th International Conference on Application of Information and Communication Technologies (AICT)* Georgia, Tbilisi, 17-19 October.

Bose, I. and Leung, A. C. M. (2013). 'The impact of adoption of identity theft countermeasures on firm value'. *Decision Support Systems,* **55** (3), pp. 753-763.

Boyd, J., Ragdell, G. and Oppenheim, C. (2007). 'Knowledge Transfer Mechanism: A case study from manufacturing'. *In Proceedings of the 8th European Conference on Knowledge Management (ECKM)* Barcelona, Spain, 6-7 September.

Brandi, U. and Elkjaer, B. (2011). 'Organizational learning viewed from a social learning perspective'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organizational Learning and Knowledge Management,* pp. 21-41. Chichester, UK, Wiley Online Library.

Bryman, A. (2012). *Social research methods,* Oxford, UK, Oxford University Press.

Bryman, A. and Bell, E. (2015). *Business Research Methods,* UK, Oxford University Press.

Cash, J. I. and Konsynski, B. R. (1985). 'IS redraws competitive boundaries'. *Harvard business review,* **63** (2), pp. 134-142.

Chenail, R. J. (2011). 'Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research'. *The Qualitative Report,* **16** (1), pp. 255-262.

Chi, L. and Holsapple, C. W. (2005). 'Understanding computer-mediated interorganizational collaboration: a model and framework'. *Journal of knowledge Management,* **9** (1), pp. 53-75.

Choo, K. R. (2011). 'The cyber threat landscape: Challenges and future research directions'. *Computers & Security,* **30** (8), pp. 719-731.

Christensen, L. T., Morsing, M. and Cheney, G. (2008). *Corporate Communications: Convention, Complexity, and Critique,* London, California, New Delhi, Singapore, SAGE Publications.

Church, N. F. (2014). 'Impact of culture on retail industry compliance'. *Journal of Business & Retail Management Research,* **9** (1), pp. 89-97.

Cifas (2016). *Future Crimes 2016 - Cifas Annual Conference 2016*. Available at:https://www.cifas.org.uk/annual_conference. Accessed: 13 April 2016.

Cifas (2015a). *Fraud 2014: what you need to know* Available at:https://www.cifas.org.uk/research_and_reports, London, UK, Cifas Leaders in fraud prevention.

Cifas (2015b). *Fraudscape: UK fraud trends*, London, UK, Cifas - The UKs Fraud Prevention Service.

Cifas (2015c). *Identity Crime*, London, UK, Cifas - The UKs Fraud Prevention Service.

Cifas (2014a). *Annual Report and Statement of Accounts 2013*, London, UK, Cifas - The UKs Fraud Prevention Service.

Cifas (2014b). *Beware what you share*, London, UK, Cifas - The UKs Fraud Prevention Service.

Cifas (2014c). *Fraudscape: Depicting the UK's fraud landscape*, London, Cifas - The UKs Fraud Prevention Service.

City of London Police (2016). *NBIF News* Available at:https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/nfib-news/Pages/default.aspx, London, UK, City of London Police.

Cohen, L. E. and Felson, M. (1979). 'Social change and crime rate trends: A routine activity approach'. *American Sociological Review,* **44** (4-August), pp. 588-608.

Cohen, W. M. and Levinthal, D. A. (1990). 'Absorptive capacity: a new perspective on learning and innovation'. *Administrative Science Quarterly,* **35** (1), pp. 128-152.

Collins, H. M. (2001). 'Tacit knowledge, trust and the Q of sapphire'. *Social Studies of Science,* **31** (1), pp. 71-85.

Cornelissen, J. (2014). *Corporate communication: A guide to theory and practice,* Sage.

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing among five approaches,* Los Angeles, London, New Delhi, Singapore, Washington DC, SAGE.

Crotty, M. (1998). *The foundation of social research: meaning and perspective in research process,* Cromwell Press, UK, SAGE Publication Limited.

Da Veiga, A. and Eloff, J. H. (2010). 'A framework and assessment instrument for information security culture'. *Computers & Security,* **29** (2), pp. 196-207.

Dale Stoel, M. and Muhanna, W. A. (2012). 'The dimensions and directionality of trust and their roles in the development of shared business–IS understanding'. *Information & Management,* **49** (5), pp. 248-256.

Dance, F. E. (1970). 'The “concept” of communication'. *Journal of Communication,* **20** (2), pp. 201-210.

Davenport, T. H. and Prusak, L. (1998). *Working knowledge: how organisations manage what they know,* Boston, MA, Harvard Business School Press.

de Crespigny, M. (2012). 'Building cyber-resilience to tackle threats'. *Network Security,* **2012** (4), pp. 5-8.

Deane-Drummond, C. (2011). *Human Identity in a Post-Darwinian World: Theological Challenges and Opportunities*. Available at:http://www.thinkingfaith.org/articles/20110408_1.htm. Accessed: 04/07 2016.

Denzin, N. K. and Lincoln, Y. S. (2011). *The SAGE handbook of qualitative research,* California, London, New Delhi, Singapore, SAGE.

DiStaso, M. W., McCorkindale, T. and Wright, D. K. (2011). 'How public relations executives perceive and measure the impact of social media in their organizations'. *Public Relations Review,* **37** (3), pp. 325-328.

Doherty, N. F., Ellis-Chadwick, F. and Hart, C. A. (1999). 'Cyber retailing in the UK: the potential of the Internet as a retail channel'. *International Journal of Retail & Distribution Management,* **27** (1), pp. 22-36.

Domaleski, J. (2000). *Building e-Commerce solutions with IBM WebSphere commerce suite and J.D. Edwards* Available at: http://www-01.ibm.com/software/info/websphere/virtualtradeshow/ecommerce/media/eIntegrator2WhitePaper.PDF, Atlanta, Georgia, CD Group, Inc.

Du, T. C., Lai, V. S., Cheung, W. and Cui, X. (2012). 'Willingness to share information in a supply chain: A partnership-data-process perspective'. *Information & Management,* **49** (2), pp. 89-98.

Easterby-Smith, M., Crossan, M. and Nicolini, D. (2000). 'Organizational learning: debates past, present and future'. *Journal of management studies,* **37** (6), pp. 783-796.

Easterby-Smith, M., Lyles, M. and Tsang, E. W. (2008). 'Inter-organizational knowledge transfer: Current themes and future prospects'. *Journal of Management Studies,* **45** (4), pp. 677-690.

Easterby-Smith, M. and Prieto, I. M. (2008). 'Dynamic capabilities and knowledge management: an integrative role for learning?’ *British Journal of Management,* **19** (3), pp. 235-249.

Easterby-Smith, M., Thorpe, R. and Jackson, P. (2012). *Management Research,* Los Angels, London, New Delhi, Singapore, Washington DC, SAGE.

Easterby-Smith, M., Thorpe, R. and Jackson, P. (2008). *Management Research,* London, California, New Delhi, Singapore, SAGE.

Easterby-Smith, M. and Lyles, M. A. (2011). 'The evolution field of organisational learning and knowledgement'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of organizational learning and knowledge management*, pp. 1-17. Chichester, U.K, Wiley.

Elyas, M., Ahmad, A., Maynard, S. B. and Lonie, A. (2015). 'Digital forensic readiness: Expert perspectives on a theoretical framework'. *Computers & Security,* **52** (2015), pp. 70-89.

Elyas, M., Maynard, S. B., Ahmad, A. and Lonie, A. (2014). 'Towards a systemic framework for digital forensic readiness.' *Journal of Computer Information Systems,* **54** (3), pp. 97-105.

Fang, S., Li, W., Yang, C. and Tsai, S. (2012). 'Managing knowledge flow in inter-organizational knowledge transfer: The dual hazard model'. *In Proceedings of the Technology Management for Emerging Technologies (PICMET)* Vancouver, Canada, July 29 to August 2 2012.

Faulkner, P. (2014). *Knowledge on trust,* Oxford, Oxford University Press.

Feledi, D. and Fenz, S. (2012). 'Challenges of Web-Based Information Security Knowledge Sharing'. *In Proceedings of the Seventh International Conference on Availability, Reliability and Security (ARES)* Prague, Czech Republic, 20-24 August.

Feledi, D., Fenz, S. and Lechner, L. (2013). 'Toward web-based information security knowledge sharing'. *Information Security Technical Report,* **17** (4), pp. 199-209.

Fenz, S., Parkin, S. and van Moorsel, A. (2011). 'A Community Knowledge Base for IT Security'. *IT Professional,* **13** (3), pp. 24-30.

Fieseler, C. and Ranzini, G. (2015). 'The networked communications manager: A typology of managerial social media impression management tactics'. *Corporate Communications: An International Journal,* **20** (4), pp. 500-517.

Finch, E. (2011). 'Strategies of adaptation and diversification: The impact of chip and PIN technology on the activities of fraudsters'. *Security Journal,* **24** (4), pp. 251-268.

Finch, E. (2007). 'Problem of Stolen Identity and the Internet'. In: Jewkes, Y. (ed.) *Crime Online,* pp. 29-43. New York, Willan Publishing.

Finch, E. (2003). 'What a tangled web we weave: Identity theft and the internet'. In: Jewkes, Y. (ed.) *Dot.cons: Crime, Deviance, and Identity on the Internet.* pp. 86-104. Cullompton, England: Willan, Willan Publishing.

Flores, W. R., Antonsen, E. and Ekstedt, M. (2014). 'Information security knowledge sharing in organisations: Investigating the effect of behavioural information security governance and national culture'. *Computers & Security,* **43** (0), pp. 90-110.

Fraud Advisory Panel (2007). *Identity fraud: do you know the signs?* London, Fraud Advisory Panel.

FTC (2013). *Taking Charge: What to do if your id is stolen* Available at: https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf, US, Federal Trade Commission.

Gaur, A. S., Mukherjee, D., Gaur, S. S. and Schmid, F. (2011). 'Environmental and Firm Level Influences on Inter-Organizational Trust and SME Performance'. *Journal of Management Studies,* **48** (8), pp. 1752-1781.

Geeta, D. V. (2011). 'Online identity theft–an Indian perspective'. *Journal of Financial Crime,* **18** (3), pp. 235-246.

Gerring, J. (2004). 'What is a case study and what is it good for?'. *American political science review,* **98** (02), pp. 341-354.

Ghaznavi, M., Perry, M., Toulson, P. and Logan, K. (2013). 'Potential Enablers of Knowledge Collaboration in Ego-centered Networks of Professionals: Transactive Memory, Trust, and Reciprocity'. *Knowledge Management: An International Journal,* **12** (1), pp. 69-83.

Ghaznavi, M., Perry, M., Logan, K. and Toulson, P. (2011). 'Knowledge Sharing in Ego-Centered Knowledge Networks of Professionals: Role of Transactive Memory, Trust, and Reciprocity'. *In Proceedings of the 8th International Conference on Intellectual Capital, Knowledge Management and Organizational Learning* Thailand, Bangkok, 27-18 October.

Glancy, F. H. and Yadav, S. B. (2011). 'A computational model for financial reporting fraud detection'. *Decision Support Systems,* **50** (3), pp. 595-601.

Glaser, B. S. and Strauss, A. (1968). 'A.(1967). The discovery of grounded theory'. *Strategies for qualitative research. London: Weidenfeld and Nicolson.*

Gottschalk, P. (2005). *Strategic knowledge management technology,* Macmillan.

Grijpink, J. (2011). 'Innovating Government: Public information infrastructures and identity fraud'. *Information Technology and Law series,* **20**, pp. 363-381.

Gummesson, E. (2000). *Qualitative methods in management research,* California, US, Sage.

Hadjielias, E. and Poutziouris, P. (2015). 'On the conditions for the cooperative relations between family businesses: the role of trust'. *International Journal of Entrepreneurial Behavior & Research,* **21** (6), pp. 867-897.

Hardy, C. (1994). *Managing strategic action: mobilizing change: concepts, readings, and cases,* Sage Publications Ltd.

Harryson, S. J., Dudkowski, R. and Stern, A. (2008). 'Transformation networks in innovation alliances–the development of Volvo C70'. *Journal of Management Studies,* **45** (4), pp. 745-773.

Hartley, J. (2004). 'Case study research'. *Essential guide to qualitative methods in organizational research,* pp. 323-333.

Hartley, D. (2013). 'What Is Social Learning Anyway?' *Chief Learning Officer,* **12** (4), pp. 18-21.

Hayes, N. (2011). 'Information technology and the possibilities for knowledge sharing'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organizational Learning and Knowledge Management*, pp. 83-104. Chichester, UK, Wiley Online Library.

Ho, M. H. and Wang, F. (2015). 'Unpacking knowledge transfer and learning paradoxes in international strategic alliances: Contextual differences matter'. *International Business Review,* **24** (2), pp. 287-297.

Home Office (2012). *Annual Fraud Indicator Report*, National Fraud Authority.

Hsiao, R., Tsai, D. and Lee, C. (2012). 'Collaborative knowing: the adaptive nature of cross-boundary spanning'. *Journal of management studies,* **49** (3), pp. 463-491.

Hsu, M., Ju, T. L., Yen, C. and 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), pp. 153-169.

Hughes, J. and Sharrock, W. (1997). *The philosophy of social research,* New York, Addison Wiley Logman Limited.

Hughes, M., Golden, W. and Powell, P. (2003). 'Inter-organisational ICT systems: The way to innovative practice for SMEs?' *Journal of Small Business and Enterprise Development,* **10** (3), pp. 277-286.

Hunter, R. (2013). *The Future of the Global Information Security*. Available at:http://public.brighttalk.com/resource/core/15901/june_13_future_of_global_info_sec_rhunter_23983.pdf. Accessed: 06/13 2013.

IBM Global Technology Services (2012). *Reputational Risk and IT: How security and business continuity can shape the reputation and value of your company,* United States of America, IBM Corporation.

IT-ISAC (2013a). *Membership Benefits* Available at:http://media.wix.com/ugd//b8fa6c_da60e7f234df0ad1e55f0e1c9695fde3.pdf, USA, Information Technology - Information Sharing and analysis Center.

IT-ISAC (2013b). *Shifting our fucus to meet new threats.* Available at:http://media.wix.com/ugd//b8fa6c_e59565238d1675b949567445f5e4baaa.pdf, USA, Information Technology- Information Sharing and Analysis Center.

Jamieson, R., Wee Land, L. P., Winchester, D., Stephens, G., Steel, A., Maurushat, A. and Sarre, R. (2012). 'Addressing identity crime in crime management information systems: Definitions, classification, and empirics'. *Computer Law & Security Review,* **28** (4), pp. 381-395.

Jansen, J. J., Van Den Bosch, F. A. and Volberda, H. W. (2005). 'Managing potential and realized absorptive capacity: how do organizational antecedents matter?'. *Academy of Management Journal,* **48** (6), pp. 999-1015.

Jasimuddin, S. M., Connell, C. and Klein, J. H. (2005). 'The challenges of navigating a topic to a prospective researcher: the case of knowledge management research'. *Management Research News,* **28** (1), pp. 62-76.

Jasimuddin, S. M., Connell, C. and Klein, J. H. (2014). 'A decision tree conceptualization of choice of knowledge transfer mechanism: the views of software development specialists in a multinational company'. *Journal of Knowledge Management,* **18** (1), pp. 194-215.

Ji, S., Wang, J., Min, Q. and Smith-Chao, S. (2007). 'Systems Plan for Combating Identity Theft-A Theoretical Framework'. *In Proceedings of the 3rd International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2007)* NewYork, USA, 8-10 October.

Junni, P. and Sarala, R. M. (2013). 'The Role of Absorptive Capacity in Acquisition Knowledge Transfer'. *Thunderbird International Business Review,* **55** (4), pp. 419-438.

Kaplow, L. and Shavell, S. (2002). 'Economic analysis of law'. *Handbook of public economics,* **3**, pp. 1661-1784.

Kaufman, F. (1966). 'Data systems that cross company boundaries'. *Harvard business review,* **44** (1), pp. 141-155.

Khan, A. (2015). 'Bitcoin–payment method or fraud prevention tool?'. *Computer Fraud & Security,* **2015** (5), pp. 16-19.

Klein, J., Connell, C. and Jasimuddin, S. (2007). 'Who needs memory? The case for the Markovian organisation'. *Knowledge Management Research & Practice,* **5** (2), pp. 110-116.

Knapp, K. J., Morris, R. F., Marshall, T. E. and Byrd, T. A. (2009). 'Information security policy: An organizational-level process model'. *Computers & Security,* **28** (7), pp. 493-508.

Knoppen, D., Christiaanse, E. and Huysman, M. (2010). 'Supply chain relationships: Exploring the linkage between inter-organisational adaptation and learning'. *Journal of Purchasing and Supply Management,* **16** (3), pp. 195-205.

Krogh, G. V. (2011). 'Knowledge sharing in organisations: The role of communities'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organizational Learning and Knowledge Management*, pp. 403-432. Chichester, UK, Wiley Online Library.

Kuhn, T. S. (1996). *The Structure of Scientific Revolutions,* Chicago, London, University of Chicago Press.

Kuhn, T. S. (1962). *The Structure of Scientific Revolution,* Chicago, the University of Chicago Press.

Kumar, K. and Van Dissel, H. G. (1996). 'Sustainable collaboration: managing conflict and cooperation in interorganizational systems'. *MIS Quarterly,* **1996** (September), pp. 279-300.

Kumar, R. (1999). *Research Methodology - A step by step guide for beginner,* London, SAGE Publication.

Kumar, V., Kumar, U. and Grosbois, D. (2007). 'Collaboration in combating identity theft'. *In Proceedings of the 2007 Administrative Sciences Association of Canada (ASAC)* Ottawa, Ontario.

Kyoung-Joo, L. (2011). 'From interpersonal networks to inter-organizational alliances for university-industry collaborations in Japan: the case of the Tokyo Institute of Technology'. *R&D Management,* **41** (2), pp. 190-201.

Lai, F., Li, D. and Hsieh, C. (2012). 'Fighting identity theft: The coping perspective'. *Decision Support Systems,* **52** (2), pp. 353-363.

Laudon, C. K. and Traver, G. C. (eds) 2013. *E-commerce 2013 business, technology, society*, Harlow, Pearson.

Lawler, S. (2008). *Identity: Sociological perspective,* Cambridge, UK, Polity Press.

Lewis, C., T. (1890). *An Elementary Latin Dictionary,* New York, Cincinnati and Chicago, American Book Company.

Lewis-Beck, M., Bryman, A. E. and Liao, T. F. (eds) 2004. *The Sage encyclopaedia of social science research methods,* California, US, Sage Publications, Inc.

Lichtenthaler, U. (2009). 'Absorptive capacity, environmental turbulence, and the complementarity of organizational learning processes'. *Academy of Management Journal,* **52** (4), pp. 822-846.

Lichtenthaler, U. and Lichtenthaler, E. (2009). 'A Capability-Based Framework for Open Innovation: Complementing Absorptive Capacity'. *Journal of Management Studies,* **46** (8), pp. 1315-1338.

Liefeld, E. (2013). *Enabling safe and secure BYOD in the enterprise with Dell KACE K Series Management Appliance*, Mountain View California, Dell Kace.

Littlejohn, S. W. and Foss, K. A. (2011). *Theories of human communication,* Long Grove, IL, Waveland Press, Inc.

Littlejohn, S. W. and Foss, K. A. (2008). *Theories of human communication,* California, USA, Lyn Uhl.

Liu, D., Ji, Y. and Mookerjee, V. (2011). 'Knowledge sharing and investment decisions in information security'. *Decision Support Systems,* **52** (1), pp. 95-107.

Lopez, V. W. B. and Esteves, J. (2013). 'Acquiring external knowledge to avoid wheel re-invention'. *Journal of Knowledge Management,* **17** (1), pp. 87-105.

LoPucki, L. (2003). 'Did Privacy Cause Identity Theft?' *Hastings Law Journal,* **54** (4), pp. 1277-1297.

Lotia, N. (2004). 'Power Dynamics and Learning in Collaborations'. *Journal of the Australian and New Zealand Academy of Management,* **10** (2), pp. 56-68.

Luoma, T., Paasi, J. and Valkokari, K. (2010). 'Intellectual property in inter-organisational relationships—Findings from an interview study'. *International Journal of Innovation Management,* **14** (03), pp. 399-414.

Mace, J., Parkin, S. and van Moorsel, A. (2010). *A Collaborative Ontology Development Tool for Information Security,* UK, Newcastle University.

Majchrzak, A. and Jarvenpaa, S. L. (2004). 'Information security in cross-enterprise collaborative knowledge work'. *Emergence: Complexity & Organization,* **6** (4), pp. 40-50.

Marciniak, R. and Bruce, M. (2004). 'Identification of UK fashion retailer use of Web sites'. *International Journal of Retail & Distribution Management,* **32** (8), pp. 386-393.

MarketLine (2015). *Online retail in the United Kingdom,* London, MarketLine.

Marshal, C. R. and Novic, S. (1995). 'Conversational effectiveness in multimedia communication'. *Information, People and Technology,* **8** (1), pp. 54-79.

Marshall, A. M. and Tompsett, B. C. (2005). 'Identity theft in an online world'. *Computer Law & Security Review,* **21** (2), pp. 128-137.

Marshall, C. and Rossman, G. B. (1995). *Designing qualitative research,* London, Sage publications.

Mason, K. J. and Leek, S. (2008). 'Learning to build a supply network: an exploration of dynamic business models'. *Journal of Management Studies,* **45** (4), pp. 774-799.

Matthews, J. and Shulman, A. D. (2000). *Questioning knowledge transfer and learning processes across R&D project teams*. Available at: http://www2.warwick.ac.uk/fac/soc/wbs/conf/olkc/archive/olk4/papers/matthews.pdf. Accessed: 07/01 2013.

McKelvey, B. (2000). 'Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft'. *UC Davis L.Rev.,* **34**, pp. 1077.

McMyler, B. (2011). *Testimony, trust, and authority,* OUP USA.

McNulty, E. (2007). 'Boss, I think someone stole our customer data'. *Harvard business review,* **85** (9), pp. 37.

Mena, C., Humphries, A. and Wilding, R. (2009). 'A comparison of inter- and intra-organisational relationships: Two case studies from UK food and drink industry'. *International Journal of Physical Distribution & Logistics Management,* **39**, pp. 762-784.

Miles, M. B., Huberman, A. M. and Saldana, J. (2014). *Qualitative Data Analysis: A Methods Soursebook,* California, London, India, Singapore, Sage Publications.

Minbaeva, D. B. (2007). 'Knowledge transfer in multinational corporations'. *Management International Review,* **47** (4), pp. 567-593.

Moran, R. (2006). 'Getting told and being believed'. *The epistemology of testimony*, pp. 272-306.

Nåden, D. (2010). 'Hermeneutics and observation–a discussion'. *Nursing inquiry,* **17** (1), pp. 75-81.

Nakano, D., Muniz, J. J. and Batista, J. E. D. (2013). 'Engaging environments: tacit knowledge sharing on the shop floor'. *Journal of Knowledge Management,* **17** (2), pp. 290-306.

National Crime Prevention Council (2005). *Preventing Identity Theft- A guide for consumers,* United States of America, National Crime Prevention Council.

NetworkingCo.Doc1. (2014). Confidential Datum - An internal Newsletter to Member only and the Author.

NetworkingCo.Doc2. (2015). Official Interactive Datum - An internal Newsletter to Members and the Author.

Newman, G. R. (2004). *Identity theft,* US Department of Justice, Office of Community Oriented Policing Services.

Newman, G. R. and McNally, M. M. (2005). 'Identity theft literature review'. *US Department of Justice, July*.

Newman, W. L. (ed.) 2005. *Social research methods,* London, Pearson.

Nonaka, I., Kodama, M., Hirose, A. and Kohlbacher, F. (2014). 'Dynamic fractal organizations for promoting knowledge-based transformation–A new paradigm for organizational theory'. *European Management Journal,* **32** (1), pp. 137-146.

Nonaka, I. and Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation,* New York Oxford, Oxford university press.

Nonaka, I., Von Krogh, G. and Voelpel, S. (2006). 'Organizational knowledge creation theory: Evolutionary paths and future advances'. *Organization Studies,* **27** (8), pp. 1179-1208.

Nonaka, I. (1994). 'A Dynamic Theory of Organizational Knowledge Creation'. *Organization Science,* **5** (1), pp. 14-37.

Noy, C. (2008). 'Sampling knowledge: The hermeneutics of snowball sampling in qualitative research'. *International Journal of social research methodology,* **11** (4), pp. 327-344.

Nylund, P. A. and Raelin, J. D. (2015). 'When feelings obscure reason: The impact of leaders' explicit and emotional knowledge transfer on shareholder reactions'. *The Leadership Quarterly,* **26** (4), pp. 532-542.

Okeke, R.I. 2015. *'The prevention of internal identity theft-related crimes: a case study research of the UK online retail companies.' published Ph. D. thesis*, University of Central Lancashire.

Oluwu, D. (2009). 'Cyber-crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa'. *Journal of Information, Law and Technology,* **1**, pp. 1-18.

Otubanjo, O. and Amujo, O. C. (2012). 'A holistic corporate identity communication process'. *The Marketing Review,* **12** (4), pp. 403-417.

Paley, J. and Eva, G. (2005). 'Narrative vigilance: the analysis of stories in health care'. *Nursing Philosophy,* **6** (2), pp. 83-97.

Panahi, S., Watson, J. and Partridge, H. (2015). 'Information encountering on social media and tacit knowledge sharing'. *Journal of Information Science,* pp. 01-13.

Panahi, S., Watson, J. and Partridge, H. (2013). 'Towards tacit knowledge sharing over social web tools'. *Journal of Knowledge Management,* **17** (3), pp. 379-397.

Park, S. and Ruighaver, T. (2008). 'Strategic approach to information security in organizations'. *In Proceedings of the Information Science and Security, 2008. ICISS. International Conference*.

PaymentCo.Doc1. (2014). Retrieval Request Report: A document-based experience from Merchant Risk Council Congress to Internal members and the Author.

PaymentCo.Doc2. (2014). UK risk monitoring TASKLIST. Weekly work schedule to Risk team and with the Author.

Peng, Y. and Sutanto, J. (2012). 'Facilitating Knowledge Sharing Through a Boundary Spanner'. *Professional Communication, IEEE Transactions on,* **55** (2), pp. 142-155.

Pérez-Nordtvedt, L., Kedia, B. L., Datta, D. K. and Rasheed, A. A. (2008). 'Effectiveness and efficiency of Cross-Border knowledge transfer: An empirical examination'. *Journal of Management Studies,* **45** (4), pp. 714-744.

Pillow, W. (2003). 'Confession, catharsis, or cure? Rethinking the uses of reflexivity as methodological power in qualitative research'. *International Journal of Qualitative Studies in Education,* **16** (2), pp. 175-196.

Pinjani, P. and Palvia, P. (2013). 'Trust and knowledge sharing in diverse global virtual teams'. *Information & Management,* **50** (4), pp. 144-153.

Polanyi, M. (1962). *Personal knowledge*, Chicago, The University of Chicago Press.

Polanyi, M. (1966). *The Tacit Dimension,* USA, the Doubleday Broadway Publishing Group.

Polanyi, M. (2003). *Personal Knowledge: Towards a Post-Critical Philosophy,* London, Routledge.

Prabowo, H. Y. (2011). 'Building our defence against credit card fraud: a strategic view'. *Journal of Money Laundering Control,* **14** (4), pp. 371-386.

Professional Security (2015). "Fraud Report", Professional Security Online Magazine, Available at: http://www.professionalsecurity.co.uk/news/interviews/fraud-report-13/. Accessed on: 17/02/2015

Rabolt, J. N. and Miler, K. J. (eds) 2009. *Concepts and cases in Retail and Merchandise Management*, New York, Fairchild Books.

Rajaguru, R. and Matanda, M. J. (2012). 'Effects of inter-organizational compatibility on supply chain capabilities: Exploring the mediating role of inter-organizational information systems (IOIS) integration'. *Industrial Marketing Management.*

Reihlen, M. and Ringberg, T. (2006). 'Computer-mediated knowledge systems in consultancy firms: Do they work'. *Research in the Sociology of Organizations,* **24**, pp. 307-336.

Ribeiro, R. and Collins, H. (2007). 'The bread-making machine: Tacit knowledge and two types of action'. *Organization Studies,* **28** (9), pp. 1417-1433.

Ringberg, T. and Reihlen, M. (2008). 'Towards a Socio-Cognitive Approach to Knowledge Transfer'. *Journal of Management Studies,* **45** (5), pp. 912-935.

Roberts, L. D. (2012). 'Cyber identity theft'. In: US Information Resource Management Association (ed.) *Cyber Crime: Concepts, Methodologies, Tools and Applications*, pp. 21-36. Unites States, Information Resource Management Association.

Roberts, L. D. (2008). *Cyber-victimisation in Australia: Extent, impact on individuals and responses,* Tasmanian Institute of Law Enforcement Studies.

Rolfe, G. (2006). 'Validity, trustworthiness and rigour: quality and the idea of qualitative research'. *Journal of advanced nursing,* **53** (3), pp. 304-310.

Rubin, H. J. and Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data,* Sage.

Rudrabasavaj, M. N. (2010). *Dynamic global: Retailing management,* Mumbai, Himalaya Publidhing House.

Ruquet, M. E. (2012). 'Study: One Method of identity Theft Trumps Cyber Threat'. *Claims,* **60** (12), pp. 9-9.

Ryan, F., Coughlan, M. and Cronin, P. (2009). 'Interviewing in qualitative research: The one-to-one interview'. *International Journal of Therapy and Rehabilitation,* **16** (6), pp. 309-314.

Saldana, J. (2009). *The Coding Manual for Qualitative Researchers,* London, Sage Publications Ltd.

Sammarra, A. and Biggiero, L. (2008). 'Heterogeneity and specificity of Inter-Firm knowledge flows in innovation networks'. *Journal of Management Studies,* **45** (4), pp. 800-829.

Sanchez, R. (2005). 'Knowledge Management and Organizational Learning'. *Fundamental Concepts for Theory and Practice*.

Saunders, M., Thornhill, A. and Lewis, P. (eds) 2015. *Research methods for business students,* Harlow, Pearson.

Schwartz, J. S., Luyckx, K. and Vignoles, L. V. (eds) 2011. *Handbook of identity Theory and Research,* London and New York, Springer.

Sekaran, U. and Bougie, R. (2013). *Research Methods for Business: A Skill-Building Approach,* West Sussex, UK, John Wiley & Sons Ltd.

Shannon, C. and Weaver, W. (1949). 'A Mathematical Model of Communication Urbana'.

Shannon, C. E. (2001). 'A mathematical theory of communication'. *ACM SIGMOBILE Mobile Computing and Communications Review,* **5** (1), pp. 3-55.

Shaw, J. D., Park, T. and Kim, E. (2013). 'A resource-based perspective on human capital losses, HRM investments, and organizational performance'. *Strategic Management Journal,* **34** (5), pp. 572-589.

Shih, S. C., Hsu, S. H. Y., Zhu, Z. and Balasubramanian, S. K. (2012). 'Knowledge sharing—A key role in the downstream supply chain'. *Information & Management,* **49** (2), pp. 70-80.

ShoppingCo.Doc1. (2014). Covert Security Operation – a one way forward in combating retail crime, presented at Retail Fraud Conference, 2014 to Author.

ShoppingCo.Doc2. (2014). “Greg’s” think piece, presented at British Retail Consortium Conference to Author.

ShoppingCo.Doc3. (2014). Fraud prevention strategy and teams' responsibilities. A talk presented at London Crime Scott, emailed to Author.

ShoppingCo.Doc4. (2014). Covert Security Operation - Retail Fraud Process. To Author.

ShoppingCo.Figure1. (2014). Group Security Structure to Author.

ShoppingCo.PPT1. (2014). Covert security operation: one way forward in combating retail crime, presented at Retail Fraud Conference, London. To Author.

ShoppingCo.PPT2. (2014). Pear-tree: operation controlled delivery, presented at London Crime Scott. To Author.

Siggelkow, N. (2007). 'Persuasion with case studies'. *Academy of Management Journal,* **50** (1), pp. 20-24.

Silverman, D. (2013). *Doing Qualitative Research:* London, SAGE Publications.

Silverman, D. (2005). *Doing Qualitative Research,* Los Angels, London, New Delhi, Singapore, SAGE Publications.

Simpson, T. W. (2013a). 'Testimony, Trust, and Authority, by Benjamin McMyler. Knowledge on Trust, by Paul Faulkner.' *Mind,* **122** (485), pp. 305-311.

Simpson, T. W. (2013b). 'Trustworthiness and Moral Character'. *Ethical theory and moral practice,* **16** (3), pp. 543-557.

Simpson, T. W. (2012). 'What is trust?' *Pacific Philosophical Quarterly,* **93** (4), pp. 550-569.

Simpson, T. W. (2011). 'e-Trust and reputation'. *Ethics and information technology,* **13** (1), pp. 29-38.

Six, F. and Sorge, A. (2008). 'Creating a High-Trust Organization: An Exploration into Organizational Policies that Stimulate Interpersonal Trust Building'. *Journal of Management Studies,* **45** (5), pp. 857-884.

Skjelsbaek, I. (2006). 'Victim and survivor: Narrated social identities of women who experienced rape during the war in Bosnia-Herzegovina'. *Feminism & Psychology,* **16** (4), pp. 373-403.

Smythe, E. A., Ironside, P. M., Sims, S. L., Swenson, M. M. and Spence, D. G. (2008). 'Doing Heideggerian hermeneutic research: A discussion paper'. *International journal of nursing studies,* **45** (9), pp. 1389-1397.

Somekh, B. and Lewin, K. (2005). *Research Methods in the Social Sciences,* London, California, New Delhi, SAGE.

Souvignet, T., Prüfer, T., Frinken, J. and Kricsanowits, R. (2014). 'Case study: From embedded system analysis to embedded system based investigator tools'. *Digital Investigation,* **11** (3), pp. 154-159.

Sproule, S. and Archer, N. (2007). 'Defining identity theft'. *In Proceedings of the Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress*.

Stahl, F., Parkin, E. S. and van Moorsel, A. (2011). *Cooperative Information Security Knowledge: Content Validation and incentives to contribute,* Newcastle upon Tyne, Newcastle University.

Stake, R. E. (2005). *Qualitative case studies.* Sage Publications Ltd.

Standage, T. (2013). "Social Networking in the 1600s", *the New York Times,* pp. SR8.

Stanford Centre for Biomedical Informatics (2016). *Protégé*. Available at: http://protege.stanford.edu/products.php#web-protege. Accessed: 01/03 2016.

Strader, T. J., Lin, F. and Shaw, M. J. (1998). 'Information infrastructure for electronic virtual organization management'. *Decision Support Systems,* **23** (1), pp. 75-94.

Styhre, A. (2011). *Knowledge Sharing in Professions: Roles and Identity in Expert Communities,* USA, Gower Publishing Ltd.

Styhre, A. (2004). 'Rethinking Knowledge: A Bergsonian Critique of the Notion of Tacit Knowledge*'. *British Journal of Management,* **15** (2), pp. 177-188.

Sullivan, C. (2009). 'Is identity theft really theft?' *International Review of Law, Computers & Technology,* **23** (1-2), pp. 77-87.

Sveiby, K. (2009). *About Karl-Eri Sveiby*. Available at: http://www.sveiby.com/about_us.html. Accessed: 07 January 2013.

Sweeney, L. (2006). 'Protecting job seekers from identity theft'. *Internet Computing, IEEE,* **10** (2), pp. 74-78.

Szulanski, G. (1996). 'Exploring Internal Stickiness: Impediments to the Transfer of Best Practice within the Firm'. *Strategic Management Journal,* **17**, pp. 27-43.

Takeuchi, H. and Shibata, T. (eds) 2006. *Moving towards a more advanced knowledge economy: Advanced knowledge creating companies,* The World Bank, Washington DC.

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M. and Rohani, V. A. (2014). 'Evaluation model for knowledge sharing in information security professional virtual community'. *Computers & Security,* **43**, pp. 19-34.

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H. and Gholipour, R. (2013). 'Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language'. *Computers & Education,* **68** (0), pp. 223-232.

Teece, D. J., Pisano, G. and Shuen, A. (1997). 'Dynamic capabilities and strategic management'. *Strategic Management Journal,* **18** (7), pp. 509-533.

The Economist (2002). *The weakest link*, The Economist Newspaper Limited.

Thomas, G. (2011). *How to do your Case Study,* London, United Kingdom, SAGE Publication Limited.

Tiwana, A. (2000). *The Knowledge Management Toolkit: Practical Techniques for Building a Knowledge Management System,* Upper Saddle River, NJ, Prentice Hall.

Travel Association (2013). *ABTA, Get Safe Online and Action Fraud warn holidaymakers: Look Before You Book*. Available from: http://www.abta.com/news-and-views/press-zone/abta-get-safe-online-and-action-fraud-warn-holidaymakers-look-before-you-bo. Accessed: December 2013.

Trustwave (2014). *2014 Security Pressure Report*.

Trustwave (2013). *Trustwave 2013 Global Security Report*. Available at: http://www2.trustwave.com/rs/trustwave/images/Trustwave_GSR_ExecutiveSummary_4page_Final_Digital.pdf. Accessed on: 20 November 2013.

Tsoukas, H. (2011). 'How should we understand tacit knowledge? A phenomenological view'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organisational learning and knowledge management,* pp. 453-476. Chichester, UK, John Wiley and Sons.

Tsoukas, H. (2005). *Complex knowledge: Studies in organizational epistemology,* Oxford, Oxford University Press.

Turville, K., Yearwood, J. and Miller, C. (2010). 'Understanding Victims of Identity Theft: Preliminary Insights'. *In Proceedings of the Cybercrime and Trustworthy Computing Workshop (CTC), 2010 Second,* 12-20 July.

Usoro, A. and Majewski, G. (2011). 'Intensive knowledge sharing: Finnish Laurea lab case study'. *Vine,* **41** (1), pp. 7-25.

Vaara, E., Sarala, R., Stahl, G. K. and Björkman, I. (2012). 'The impact of organizational and national cultural differences on social conflict and knowledge transfer in international acquisitions'. *Journal of Management Studies,* **49** (1), pp. 1-27.

van Riel, C. B. M. (1995). *Principles of Corporate Communication,* Great Britain, Prentice Hall.

van Riel, C. B. (2013). 'Corporate reputation and the discipline of public opinion'. *The handbook of communication and corporate reputation,* pp. 11À19.

van Riel, C. B. and Fombrun, C. J. (2007). *Essentials of corporate communication: Implementing practices for effective reputation management,* Routledge.

Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M. and Baesens, B. (2015). 'APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions'. *Decision Support Systems,* **75**, pp. 38-48.

Van Wijk, R., Jansen, J. J. and Lyles, M. A. (2008). 'Inter-and Intra-Organizational Knowledge Transfer: A Meta-Analytic Review and Assessment of its Antecedents and Consequences'. *Journal of Management Studies,* **45** (4), pp. 830-853.

van Wijk, R., van den Bosch, F. and Volberda, H. (2011). 'Organizing Knowledge in Social, Alliance, and Organizational Networks'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organisational learning and knowledge management,* pp. 477-504. Chichester, UK, John Wiley and Sons.

van Woerkum, C. and Aarts, N. (2008). 'Staying connected: The communication between organizations and their environment'. *Corporate Communications: An International Journal,* **13** (2), pp. 197-211.

Vance, A., Siponen, M. and Pahnila, S. (2012). 'Motivating IS security compliance: insights from habit and protection motivation theory'. *Information & Management,* **49** (3), pp. 190-198.

Verčič, A. T., Verčič, D. and Sriramesh, K. (2012). 'Internal communication: Definition, parameters, and the future'. *Public relations review,* **38** (2), pp. 223-230.

VeriSign (2012). *Establishing a Formal Cyber Intelligence Capability: A VeriSign iDefence Security Intelligence Services*. Available at: https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf. Accessed: 20 February 2013.

Verona, G. and Zollo, M. (2011). 'The human side of dynamic capabilities: a holistic learning model'. In: Easterby-Smith, M. and Lyles, M. A. (eds.) *Handbook of Organizational Learning and Knowledge Management,* pp. 535-550. Chichester, UK, Wiley Online Library.

Vrakas, N. and Lambrinoudakis, C. (2013). 'An intrusion detection and prevention system for IMS and VoIP services'. *International Journal of Information Security,* **12** (3), pp. 201-217.

Walsham, G. (2001). 'Knowledge Management: The Benefits and Limitations of Computer Systems'. *European Management Journal,* **19** (6), pp. 599-608.

Wang, S. and Noe, R. A. (2010). 'Knowledge sharing: A review and directions for future research'. *Human Resource Management Review,* **20** (2), pp. 115-131.

Wang, W. J., Yuan, Y. and Archer, N. (2006). 'A contextual framework for combating identity theft'. *Security & Privacy, IEEE,* **4** (2), pp. 30-38.

Wei, Y. (2010). 'Analysis on influencing factors of tacit knowledge sharing and solutions for high-tech enterprises'. *In Proceedings of the 3rd IEEE International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII)* Xi'an, China, 26-28 November.

Welch, M. (2006). 'Rethinking relationship management: exploring the dimension of trust'. *Journal of Communication Management,* **10** (2), pp. 138-155.

Welch, M. and Jackson, P. R. (2007). 'Rethinking internal communication: a stakeholder approach'. *Corporate Communications: An International Journal,* **12** (2), pp. 177-198.

Wenger, E. (1998). 'Communities of practice: Learning as a social system'. *Systems thinker,* **9** (5), pp. 2-3.

Wilhelm, W. K. (2004). 'The fraud management lifecycle theory: a holistic approach to fraud management'. *Journal of economic crime management,* **2** (2), pp. 1-38.

Wilson, T. D. (2002). 'The nonsense of knowledge management'. *Information research,* **8** (1).

Wright, D. and Hinson, M. (2010). 'How new communications media are being used in public relations: A longitudinal analysis'. *Public Relations Journal,* **4** (3), pp. 1-27.

Xu, Z. (2012). 'Victimized by Phishing: A Heuristic-Systematic Perspective'. *Journal of Internet Banking and Commerce,* **17** (3), pp. 1-16.

Yang, T. and Maxwell, T. A. (2011). 'Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors'. *Government Information Quarterly,* **28** (2), pp. 164-175.

Yin, R. K. (2012). *Applications of Case Study Research,* London, SAGE publications.

Yin, R. K. (2009). *Case Study Research: Design and Methods,* USA, SAGE Publication, Inc.

Appendix 1 Letter of Invitation

Invitation

Dear Sir or Madam:

I am writing to invite you to participate in information security research via answering a questionnaire. The research is covering online frauds and risk associated with online shopping and explores how companies can improve their fraud, risk, compliance and other information security practices by sharing their knowledge and expertise with peers in other organisations.

The online identity related fraud is a common problem for food and grocery retailers such as Tesco, Asda, Sainsbury's and Morrison's. There is no immediate benefit to your organisation of this participation. However, the insights acquired from your participation will be compared and contrasted with other similar companies. These results will help you asses where your company is and which areas still need consideration to improve.

Your participation will help towards fulfilling partial requirement for a doctoral degree. Any personal information of participants will be kept confidential and participants and their associated companies will be represented as X, Y, Z to ensure anonymity. You have full choice to withdraw from your participation any time during the study. The interview takes approximately 40 minutes. On request, we will provide you with a summary of the results.

The research group will be pleased to answer any question and concerns that you may have about this study. I have listed the contact details of investigators involved in the project:

Principal Investigator:

Rozina Chohan (Doctoral Researcher)
Rchohan1@uclan.ac.uk (Mobile: 07939918049)

Other team members:

1. Dr Mahmood Shah (Director of Studies)
MHShah@uclan.ac.uk (Mobile: 07737179399)
2. Dr Mary Welch (Research supervisor)
MWelch@uclan.ac.uk (Office: 01772 89 4753)
3. Dr Mitchell Larson (Research supervisor)
MJLarson@uclan.ac.uk (Office: 01772 89 4685)

I look forward to your reply and the opportunity of working with you.

Kind Regards
Rozina Chohan
Lancashire Business School,
University of Central Lancashire,
Preston PR1 2HE

Appendix 2 Interview Schedule

Individual questions

Block 1# Interview Schedule Introduction

QNo.	Example questions	Probing questions	Source	Rationale
1	What is your job title?	-What does this involve? -How long have you been doing these duties? -What process of fraud cycle are you involved? Threat deterrence, prevention, detection, mitigation, analysis, policy, investigation, or any other? Please specify! -What are the main day-to-day activities that you perform? -Is there any special project(s) that you are involved?	Wilhelm, 2004	These questions are asked to explore security measures employed by the organisation. These questions are based on fraud management life cycle (Wilhelm, 2004) and addressed research objective 1(OBJ1) to evaluate security measures employed by the retailers.
2	-Are you involved in technical work such as encryption, filtration or something else? -What skills are needed for this role? -How did you acquire these skills?	Does this work make application of technical skills gained through experience or something already captured in a document or database?	Security professional may have fluid mix of knowledge with a combination of technical (encryption, decryption and password protection) and strategic (policymaking) skills. These questions with its probes will help to seek their nature of knowledge.	These questions help to address elements of the applied framework (nature of knowledge). These questions explicitly help to achieve research objectives (OBJ4 and RQ5) to evaluate and extend the applied framework. Thus, contributes to the conceptual framework.

3	-What security threats do you deal in your organisation? -Do you deal customers data theft, intellectual property theft, reputation damage, fines or legal actions (or any other tasks)? Please specify	-How do you deal with these threats? -Do you deal them independently or you work as a team?	Trustwave, 2014, p. 7	These questions and the probes help to address research (OBJ1) specifically. To assess their knowledge about current security treats faced by retailers. However, some aspects also support research objective (OBJ5) to evaluate whether their internal communication is active or isolated contributes to conceptual framework.

Block 2# Questions on Inter-organisational Knowledge Sharing Structures and Mechanisms

QNo.	Example questions	Probing questions	Source	Rationale
4	As a member of professional institute what are the other relevant institutes in retail or online security in your surroundings? For example: Next, Sports Direct, Debenhams etc.	Would you list relevant professional institutes?	No source	These questions are asked to assess their own knowledge of similar organisations. This question is asked to create a situation that assist exploration of inter-organisational knowledge sharing. If they are aware of the similar organisations, there is possibility that they know their peers in these organisations. Thus it contributes to research objectives (OBJ4 and OBJ5)
5	Do you share best practices or lessons learned from your experience with the people	If yes:	Easterby-Smith, Lyles and Tsang, 2008; Panahi, Watson and Partridge, 2013	This question with probes contributes to an element of the conceptual framework discussed (Chapter 3, Section

	belong to any of these or other organisations?	(1) How do you interact with people in other organisations? (2) Do you use face-to-face or IT-assisted mechanism to communicate with each other? Why? (3) What is your relationship with your peers in other organisations? Does this relation affect your learning? If so, how? (4) Do you communicate with them directly or through someone's help such as manager or colleague? (5) Which mechanisms do you use that are IT-assisted (i.e. email, SharePoint, online real time meetings, blogs, discussion forums, video conferencing, or any other? Why? (6) Which mechanisms do you use from face-to-face interactions (i.e. interpersonal interaction, discussion, social gathering, organised meetings, presentations, reports etc.)? Why? (7) Do you share white papers, industry specific magazines, or newsletters with each other?		3.4.3). The rationale behind these questions is to explore the structures and mechanisms officials use to gain an external knowledge and their own opinion about these constructs. This question is particularly focusing partnership (Chapter 2, Section 2.5.2). These questions contributes to RQ2 which seeks to find extent to which partnership works between the organisations and contributes to research objective (OBJ4 and OBJ5) the conceptual framework
6	Have you been provided membership with any professional body/community	If yes: (1) Would you please list these communities?	Many famous retailers (i.e. IBM, NAB, and Nokia) use professional security forums (i.e. ISF, Gartner, and ISAC) to gain an external knowledge from global peers.	This question contributes to RQ1 that seeks to explore what is working and what does not seem to provide benefit in terms of knowledge

	such as ISF or IT-ISAC security forums?	(2) How useful these security forums are in terms of improving your knowledge and skills?	These questions are asked to explore whether retailers in the UK use any of these forums by subscription to improve their knowledge.	shared by networking forums. This also contributes to conceptual framework – the structure element. (Chapter 3, Section 3.4.3). This question is particularly focusing fraud forums discussed in Chapter 2 (Section 2.5.3). It contributes to OBJ 4 and OBJ 5
7	Are you registered with any other virtual community related to your area to extract knowledge on recent trends? For example: Information System Security Association (ISSA), Information Security Professional Association (ISPA), LinkedIn security Group, Society of Information Risk Analysts (SIRA), please specify	If yes: (1) How often do you communicate within network? (2) Is it effective and beneficial to learn from that network? (3) Who manages it? (4) Do you receive a prompt response when you ask a query in that network?	Tamjidyamcholo *et al.*, 2013	OBJ 4 and OBJ 5 This contributes to RQ3 that seeks to explore why some individual have less active participation in information security knowledge using virtual communities This also contributes to conceptual framework – the structure element. This question is particularly focusing virtual communities (Chapter 2, Section 2.5.4)
8	How do you compare the knowledge sharing process within your organisation and with external organisations in terms of relationships, accessibility, and mechanisms used?	Which one do you more frequently use over the other and why?	Mena, Humphries and Wilding, 2009	To assess relationships status and degree of interaction with internal and external peers (Chapter 3, Section, 3.3.3)

09	How do you feel about your overall experience of knowledge sharing process?	Would you like to have more open lines of communication with people in other organisations? What factors might prevent this from happening? Is there anything that you can do to overcome those barriers?		To assess their own view of situation and their feelings of power (powerlessness) about the knowledge sharing process

Block 3# Questions on Nature of Knowledge and Accuracy

QNo.	Example questions	Probing questions	Source	Rationale
10	Is it difficult to share real experience electronically?	If yes, do you manage it? How? How and what extent are IT-assisted tools effective in facilitating tacit knowledge sharing? What are the capabilities of these tools and what are the barriers (i.e. technical, legal, motivational) for tacit knowledge sharing? What is needed to improve the capacity of IT tools?	Nonaka and Takeuchi, 1995; Panahi, Watson and Partridge, 2013	OBJ4 and OBJ5 To assess whether knowledge accuracy concerns matters when involves tacit knowledge and the extent to which digital communication supports its sharing (Chapter 3, Section 3.5)
11	Do you find yourself sharing or explaining the same thing in different ways to aid your colleague's understanding?	What are the differences between face to face versus online tacit knowledge sharing? Which one do you prefer?		This question is used to assess their alternative techniques useful to ensure knowledge accuracy and thus contributes to nature of knowledge from conceptual framework.

Block 4# Questions on Trust and Risk

QNo.	Example questions	Probing questions	Source	Rationale
12	Do you usually trust the content that your peers have shared with you?	How do you measure its reliability? Do you apply it in performing your own specialised tasks?	Tamjidyamcholo *et al.*, 2013	Contributes to RQ2, RQ3, OBJ4, and OBJ5 by exploring elements associated to trust and risk (Chapter 3, Section 3.4.2). To assess trust associated to shared content.
13	Would you consider any information that you share with other organisations to be sensitive?	Do you need permission from your line manager before you share anything with the people in other organisations? Do you consider that people in other organisations will misuse sensitive information if you share documents, blueprints or hardware?	Easterby-Smith, Lyles and Tsang, 2008; Majchrzak and Jarvenpaa, 2004	To assess risk associated with collaboration process such as leaking confidential information (Chapter 2, Section 2.5).
14	Have you had any experience that makes you reluctant to share your knowledge?	Why?	Junni and Sarala, 2013	To explore employee negative reaction. Inferiority feeling of having insufficient knowledge (Chapter 3, Section 3.3.3).

Block 5# Questions on Knowledge Absorptive Capacity

QNo.	Example questions	Probing questions	Source	Rationale
15	Do you need previous related knowledge to learn from your peers?	If yes, what do you do to obtain it?	Lichtenthaler and Lichtenthaler, 2009; Cohen and Levinthal, 1990	This covers OBJ5, extension of framework, element of inter-organisational dynamisms (i.e. knowledge absorptive capacity)
16	Do you think that the knowledge that your peers have shared with you is valuable and beneficial to you? How do you know?	What do you do with the knowledge once you receive from your peers? Do you typically share it with other colleagues in your team?		This question with probes assesses value from external knowledge and consider the element of verified source of knowledge.

Managerial questions

Block 6# Questions on Managerial Related Further Exploration

QNo.	Example questions	Probing questions	Source	Rationale
1	Do you share your knowledge and expertise with managers in other organisations?	If yes, what is that knowledge is about? Is that knowledge related to strategy or policy making for information security or something else?	Ahmad, Maynard and Park, 2014	This question will help to assess nature of knowledge (OBJ4 and OBJ5) evaluation and extension of the proposed framework
2	What motivates you to share knowledge with other organisations?	What are the incentives for your contribution in the knowledge sharing process? Where do these incentives come from	Stahl, Parkin and van Moorsel, 2011, Techanical Report Series, Newcastle University	This question contributes to assessing incentive useful to motivate knowledge sharing process (Chapter 3, Section 3.3.3)

3	Which mechanism do you prefer to share your knowledge?	Is there any cost and benefit related to these mechanisms?	Barringer and Harrison, 2000, p. 380	To assess cost and benefits associated with knowledge sharing process.
4	Who are the knowledge collaborators? Are they your supplier, partner, buyer, competitor or someone else from your community or circle? Please specify	On what basis do you select your knowledge partners (accuracy or reliability)?	Easterby-Smith, Lyles and Tsang (2008)	Companies also use buyer, supplier and partner to explore external knowledge To assess their knowledge about their knowledge contributors and relationships dependency. This question contributes to conceptual framework by focusing power relation. Therefore, may help OBJ4 and OBJ5.
5	Does the geographical location of your partner hinder your collaboration?	If yes, how do you manage it? Do you see each other face-to-face? How often do you meet?	ISF chapter meeting mechanism provides opportunities to members in the same geographic region to meet and discuss security related issues, which gave base to this question. This is also consistent with Almeida, Hohberger and Parada (2011). These authors believed that geographically mediated organisations support to generate informal social ties to fluidly share knowledge.	To assess geographically mediated social ties and difficulty associated with knowledge sharing with peer at distant location.
6	Do you collaborate with anyone who is willing to share knowledge? Do you limit yourself to equal size organisations and with people in the similar domain?	If yes, how do you balance levels of knowledge and competency? Do you or your team need extra training programs to be able to gain knowledge?	Polanyi (1962) supported that having familiarity with similar theoretical knowledge improves knowledge holders' interpretation. Styhre (2011) also supports the use patterns from similar domain of knowledge.	To assess whether their choice of collaborator matters by considering level of competency or the domain specific partner is important (Chapter 2, Section 2.3.2)
7	Do you need special contact with managers in the other organisations to create	-Why?	Easterby-Smith, Thorpe and Jackson, 2008	This question assesses power or dependency relations and

	collaborative environment or previous relations are enough?	-How do you facilitate productive knowledge sharing in your organisations?		contributes to OBJ4 and OBJ5
8	Do you encourage your team members to share their knowledge? If so, how?	If yes, how do you measure your team member's contribution to extend the knowledge? Do you consider incentives (i.e. promotions or rewards) to improve their levels of satisfaction and motivation in the knowledge contribution?	Nakano, Muniz and Batista, 2013, p. 290	OBJ4 and OBJ5 To assess company characteristics, framework evaluation. To know managerial efforts in encouraging team members' motivation to contribute their knowledge (Chapter 3, Section 3.3.3)
09	Which among these mechanisms do you use to share knowledge with other organisations? (Transfer experienced professionals, plan social activities, training members of recipient firms or sharing blueprints or hardware)	Why? Do you consider training members of recipient firms or planning socialize activities as costly mechanisms? -Do you need a considerable time and cost for the chosen mechanisms? - What are the potential benefits from this process?	Easterby-Smith, Lyles and Tsang, 2008, p. 682; Almeida, Hohberger and Parada, 2011	To understand chosen managerial mechanism and value form the knowledge sharing process.
10	Is it risky to transfer document, blueprint or hardware?	How do you measure these risk?	The issue of risk is already discussed in block 4, question 13	
11	What do you do with the knowledge you learnt from managers in other organisations?	Whom do you share it in your organisation?		To address intra-organisational collaboration This question will support on element of adopted framework (i.e. intra-

			organisational knowledge sharing capability and intention)
12	Is there anything else that you might think is useful to share about this research		

Appendix 3 Coding Manual

Coding Manual Hierarchy: Security Measures

Identity theft prevention measures					
Main Code	***Category 1***	***Category 2***	***Deduced***	***Induced***	***Source***
Covert security operation	Internal support	Top Management	X		Okeke, 2015; Elyas *et al.*, 2014
		Information Security	X		Ahmad, Maynard and Park, 2014; Wilhelm, 2004; Elyas *et al.*, 2014
	External support	Police		X	ShoppingCo, PaymentCo, NetworkingCo
		Agencies		X	ShoppingCo, PaymentCo, NetworkingCo
		Courier		X	ShoppingCo
	Outsourcing support	Consultancy Software Anti-phishing		X	ShoppingCo
Transaction monitoring				X	PaymentCo

Coding Manual Hierarchy: Knowledge Sharing and Communication

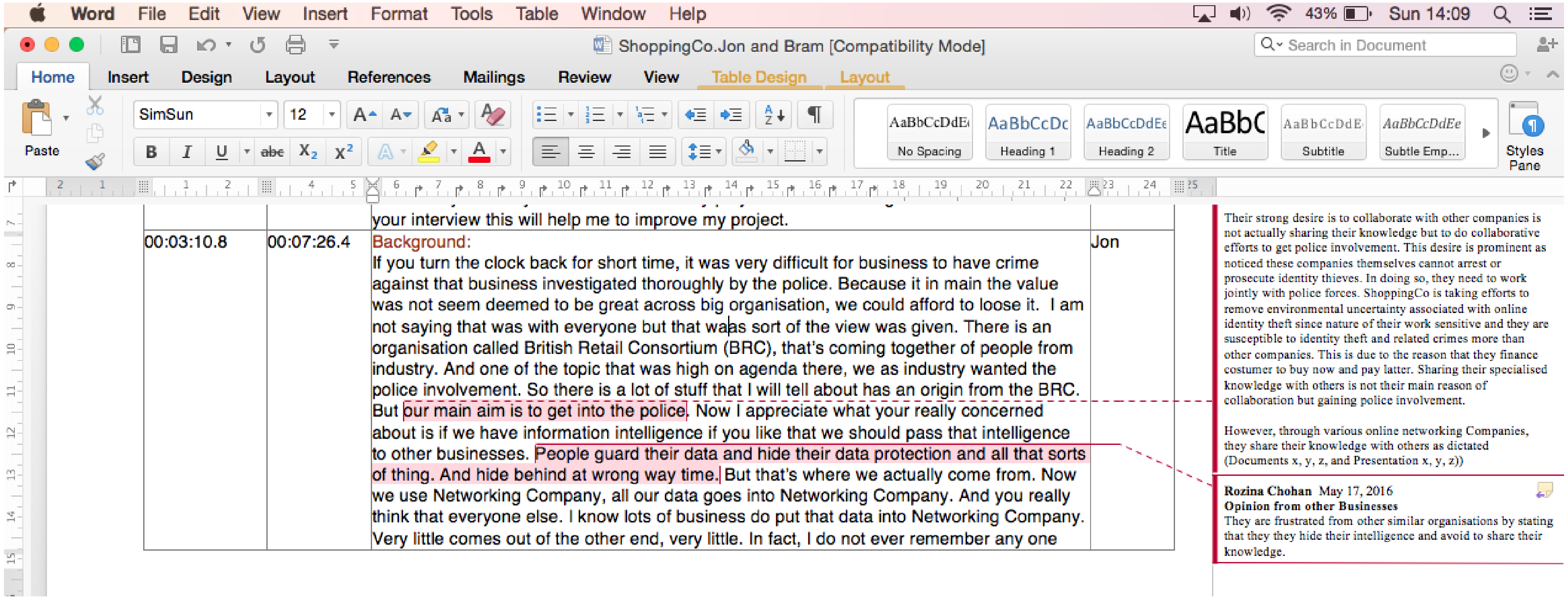
Inter-organisational knowledge sharing

Main Code	***Category 1***	***Category 2***	***Category 3***	***Category 4***	***Deduced***	***Induced***	***Source***
Characteristics of Firm	Absorptive capacity	Relevant experience			X		Cohen and Levinthal, 1990; Junni and Sarala, 2013; Jansen, Van Den Bosch and Volberda, 2005
		Training			X		Elyas *et al.*, 2014; Nakano, Muniz and Batista, 2013
		Competitive staff			X		Almeida, Hohberger and Parada, 2011; Lichtenthaler and Lichtenthaler, 2009; Harryson, Dudkowski and Stern, 2008
		Valuable knowledge			X		Pérez-Nordtvedt *et al.*, 2008
	Intra transfer capability	Company intranet			X		Argenti, 2013
		Social Media			X		DiStaso, McCorkindale and Wright, 2011; Wright and Hinson, 2010
		Negative reaction Or internal risk			X		DiStaso, McCorkindale and Wright, 2011; Nakano, Muniz and Batista, 2013
	Motivation	Incentives			X		Feledi, Fenz and Lechner, 2013
		Rewards and appreciation,				X	ShoppingCo

		personal satisfaction					
Interactive dynamisms	Power relations				X		Easterby-Smith, Lyles and Tsang, 2008
	Structures & Mechanisms	Formal structure	Partnership	Digital	X		Flores, Antonsen and Ekstedt, 2014; Liu, Ji and Mookerjee, 2011
				Offline	X		
			Forums	Digital	X		Gartner, ITISAC, ISF
				Offline	X		Gartner, ITISAC, ISF
			Virtual communities		X		Tamjidyamcholo *et al.*, 2014
		Informal Structure / Social ties	Past colleagues		X		Almeida, Hohberger and Parada, 2011
			Friends		X		Easterby-Smith, Lyles and Tsang, 2008
	Trust and Risk	Reputational damage			X		Professional Security, 2015
		Leakage/ Loss of sensitive customers i.e. Payroll and customer information			X		Ahmad, Bosua and Scheepers, 2014; Majchrzak and Jarvenpaa, 2004 ShoppingCo, PaymentCo
		Confidentiality				X	ShoppingCo, PaymentCo, NetworkingCo

		Abuse of knowledge				X	Becerra, Lunnan and Huemer, 2008
		Loss of valuable knowledge			X		Ahmad, Bosua and Scheepers, 2014
Nature of knowledge	Degree of tacitness	Degree of tacitness			X		Easterby-Smith, Lyles and Tsang, 2008
	Comprehension				X		Tsoukas, 2011; Nonaka *et al.*, 2014; Styhre, 2004
	Accuracy				X		Panahi, Watson and Partridge, 2013; Panahi, Watson and Partridge, 2015
Exploration v/s Exploitation	Balance					X	ShoppingCo, PaymentCo and NetworkingCo
Retailers-police relationships						X	ShoppingCo
Outcrossing organisations						X	ShoppingCo, PaymentCo

Appendix 4 Transcript Coding

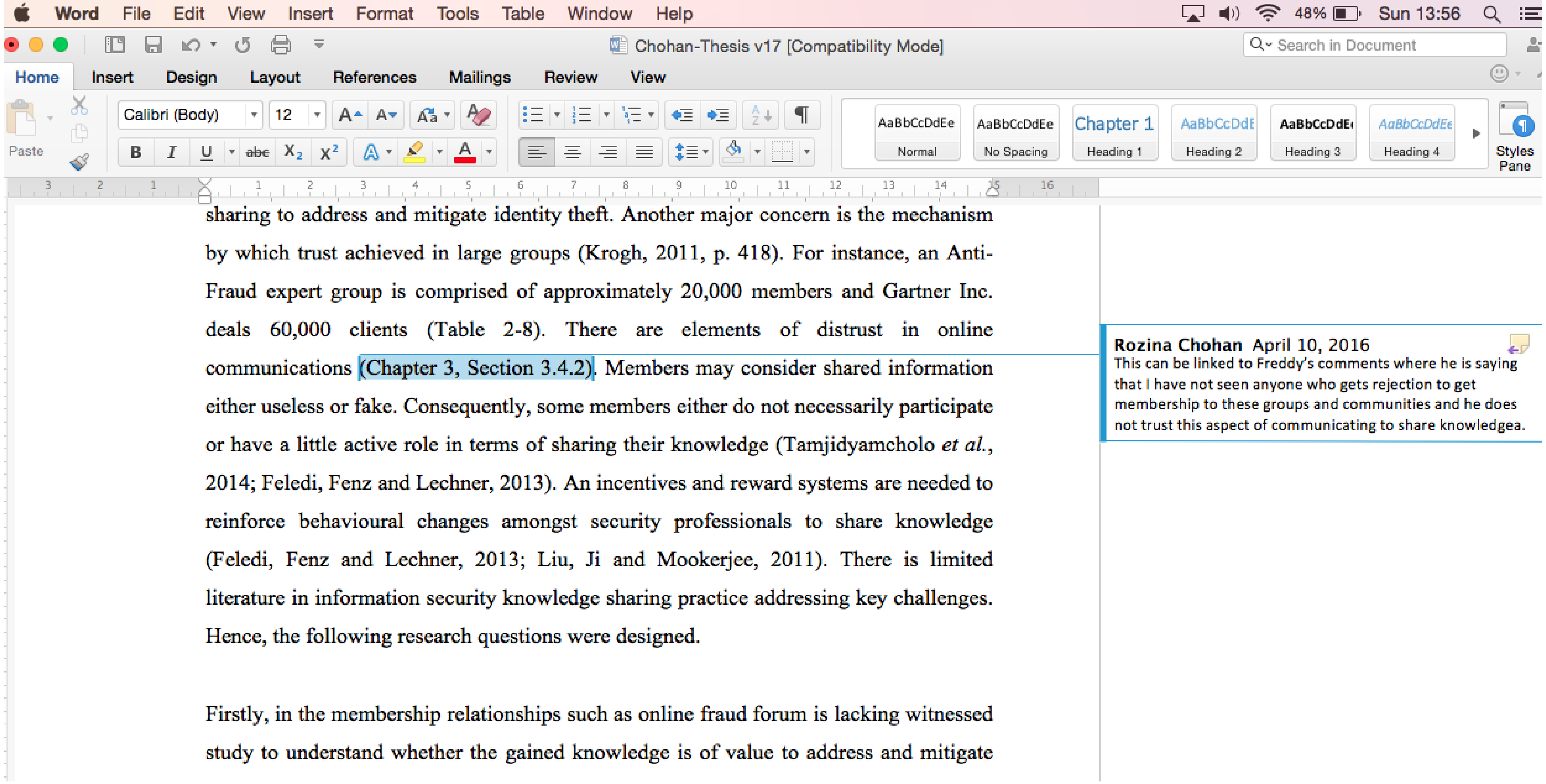

Word File Edit View Insert Format Tools Table Window Help
43% Sun 14:09
ShoppingCo.Jon and Bram [Compatibility Mode]
Search in Document
Home Insert Design Layout References Mailings Review View Table Design Layout
Paste
SimSun 12
AaBbCcDdE No Spacing
AaBbCcDc Heading 1
AaBbCcDdEe Heading 2
AaBbC Title
AaBbCcDdE Subtitle
AaBbCcDdEe Subtle Emp...
Styles Pane

		your interview this will help me to improve my project.	
00:03:10.8	00:07:26.4	Background: If you turn the clock back for short time, it was very difficult for business to have crime against that business investigated thoroughly by the police. Because it in main the value was not seem deemed to be great across big organisation, we could afford to loose it. I am not saying that was with everyone but that waas sort of the view was given. There is an organisation called British Retail Consortium (BRC), that's coming together of people from industry. And one of the topic that was high on agenda there, we as industry wanted the police involvement. So there is a lot of stuff that I will tell about has an origin from the BRC. But our main aim is to get into the police. Now I appreciate what your really concerned about is if we have information intelligence if you like that we should pass that intelligence to other businesses. People guard their data and hide their data protection and all that sorts of thing. And hide behind at wrong way time. But that's where we actually come from. Now we use Networking Company, all our data goes into Networking Company. And you really think that everyone else. I know lots of business do put that data into Networking Company. Very little comes out of the other end, very little. In fact, I do not ever remember any one	Jon

Their strong desire is to collaborate with other companies is not actually sharing their knowledge but to do collaborative efforts to get police involvement. This desire is prominent as noticed these companies themselves cannot arrest or prosecute identity thieves. In doing so, they need to work jointly with police forces. ShoppingCo is taking efforts to remove environmental uncertainty associated with online identity theft since nature of their work sensitive and they are susceptible to identity theft and related crimes more than other companies. This is due to the reason that they finance costumer to buy now and pay latter. Sharing their specialised knowledge with others is not their main reason of collaboration but gaining police involvement.

However, through various online networking Companies, they share their knowledge with others as dictated (Documents x, y, z, and Presentation x, y, z))

Rozina Chohan May 17, 2016
Opinion from other Businesses
They are frustrated from other similar organisations by stating that they they hide their intelligence and avoid to share their knowledge.


Word File Edit View Insert Format Tools Table Window Help
48% Sun 13:56
Chohan-Thesis v17 [Compatibility Mode]
Search in Document
Home Insert Design Layout References Mailings Review View
Paste
Calibri (Body) 12
Normal No Spacing Heading 1 Heading 2 Heading 3 Heading 4
Chapter 1
Styles Pane

sharing to address and mitigate identity theft. Another major concern is the mechanism by which trust achieved in large groups (Krogh, 2011, p. 418). For instance, an Anti-Fraud expert group is comprised of approximately 20,000 members and Gartner Inc. deals 60,000 clients (Table 2-8). There are elements of distrust in online communications (Chapter 3, Section 3.4.2). Members may consider shared information either useless or fake. Consequently, some members either do not necessarily participate or have a little active role in terms of sharing their knowledge (Tamjidyamcholo *et al.*, 2014; Feledi, Fenz and Lechner, 2013). An incentives and reward systems are needed to reinforce behavioural changes amongst security professionals to share knowledge (Feledi, Fenz and Lechner, 2013; Liu, Ji and Mookerjee, 2011). There is limited literature in information security knowledge sharing practice addressing key challenges. Hence, the following research questions were designed.

Firstly, in the membership relationships such as online fraud forum is lacking witnessed study to understand whether the gained knowledge is of value to address and mitigate

Rozina Chohan April 10, 2016
This can be linked to Freddy's comments where he is saying that I have not seen anyone who gets rejection to get membership to these groups and communities and he does not trust this aspect of communicating to share knowledgea.

Appendix 5 Publications

Parts of this thesis are published in these papers:

- In abstract of Conference 'Research Now' at University of Central Lancashire, 2014 2014

- In abstract of Fourth Annual Research Student Conference at University of Central Lancashire, 2014

- Overcoming Trust Barriers: Evaluating Inter-Organisational Knowledge Sharing in UK Online Retail Sector. *Proceedings of the 15th European Conference on Knowledge Management*, the Santarem School of Management and Technology, Polytechnic Institute of Santarem, Portugal, 4-5 September 2014, Volume 3