Identity theft prevention in online retail organisations: a knowledge sharing framework

Abdullah [1, 2],
Mahmood Hussain Shah[1]
Waqar Ahmed[3]
[1] School of Business, University of Central Lancashire, Preston, PR1 2HE, UK
[2] Department of Computer Science, Shah Abdul Latif University, Khairpur, Sindh, Pakistan
[3] School of Medicine, University of Central Lancashire, Preston PR1 2HE, UK

Keywords
Knowledge Management, Knowledge Transfer, Identity Theft Prevention, Information System, Information Security, Case Study Research.

Abstract
This research investigates knowledge transfer processes within online retail organisation to prevent identity theft. An analysis of the ways in which individuals and teams transfer identity theft prevention knowledge within the organisation is presented. A qualitative case study research approach using guiding framework proposed by Salleh (2010) was adopted and extended to improve identity theft prevention knowledge sharing processes in online retail organisations. Fourteen one-to-one semi-structured interviews were conducted. Internal documents from a leading online retailer in the UK were also analysed. Research shows that knowledge regarding identity theft prevention is not being shared and individuals are learning from their own experiences which is time consuming. Existing knowledge transfer barriers in the organisation were identified and improvements in knowledge sharing processes within the retail industry in the UK are proposed. Only one case study has been investigated and further case studies need to be conducted in different organisations and internationally and a cross-comparisons conducted. This study provides managers with useful information in developing appropriate training systems to educate staff on sharing institutional knowledge to prevent identity theft. This research provides new insights into identity theft prevention by extending an existing framework proposed by Salleh (2010) in terms of enhancing knowledge transfer process to prevent identity theft in the retail industry.

1. Introduction

The retail industry is afflicted by identity (ID) theft related to on-line transactions. Enhanced awareness and media reports of ID theft such as stealing bank account details, credit or debit card information and other valuable personal information has increased the fear to public related to on-line shopping and banking. The governments and research groups are focused on understanding and solving issues of ID fraud and therefore conducting parallel research projects in this arena. (Shaobo Ji *et al.*, 2007). This research aims to study, analyse and propose solutions for sharing knowledge regarding ID theft prevention in the UK retail industry. Existing barriers in the knowledge transfer process of ID theft prevention among individuals and departments have been investigated. The framework proposed by Salleh (2010) for improving ID theft prevention knowledge sharing inside these organisations has been adopted and extended to apply to the retail industry.

2. Background

ID theft has become common in businesses and in banking sector particularly related to online transactions and retail purchasing (Fennelly, 2012; Clough, 2015). It is one of the fastest

growing crimes in the world (Grover *et al.*, 2011). Organisations and government institutions have implemented policies and standards to stop ID fraud (Soomro *et al.*, 2016; Israilidis *et al.*, 2015). Despite such measures the rate of ID theft crimes is increasing due to the explicit nature of knowledge sharing in the form of policies and standards. Most workers do not follow policies or do not even read policy and security related documents (Aimeur *et al.*, 2011). Hence, these instances could be reduced by incorporating knowledge management (KM) within organisations (Conrad *et al.*, 2012).

Therefore, at the moment KM is a major focus of research in different disciplines (Musulin *et al.*, 2011; Li and Kuan, 2015). Particularly knowledge sharing in rapidly growing industries such as e-marketing, telemarketing, e-banking, project management and e-commerce. An important concept with KM is tacit knowledge, gained by doing things and experiencing them (Guang-bin *et al.*, 2010). In 2010, Salleh developed a model for sharing tacit knowledge in a public sector accounting organisation. Developed model connected the knowledge holders' process of sharing within accounting organisations.

Surveys and case studies (Bindra *et al.*, 2012; CIFAS, 2012; CIFAS, 2013; Sakharova, 2012; Bradford and Cundiff, 2006; Lai *et al.*, 2012; Romanosky *et al.*, 2011; Stephen, 2013) have been conducted to understand ID theft. Various categories of ID theft, frauds and crimes are being committed by thieves and the different methods are used to commit ID related frauds (Sakharova, 2012; Lai *et al.*, 2012; Jin *et al.*, 2011; Bilge *et al.*, 2009; Fire *et al.*, 2013; Bose and Leung, 2013; Reyns, 2013). Very little work on knowledge sharing concepts recognise that tacit

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

Table 1: Comparison of Related Frameworks

knowledge sharing has been applied in the context of ID theft prevention. Personal information is still being stolen, and organisations are not fully capable of preventing information of related persons from being stolen. Companies are being victimised and thus suffer large financial losses. This study has investigated and analysed knowledge transfer processes within online retailing in the UK and proposes practical improvements to the process of knowledge sharing to prevent ID theft within organisations. Various frameworks have been studied in the literature such as Arachchilage *et al.,* (2012), Trkman and Desouza, (2012), Yan Li and Zetian Fu ,(2007), Amin and Hussain, (2010), WenJie Wang and Yufei Yuan (2006), Noor and Salim, (2012), and Salleh, (2010) (see Table 1).

Comparative analysis of knowledge sharing and ID theft prevention enabled the conceptual framework proposed by Salleh (2010) to be chosen as a guiding framework for data collection. It has been adopted and matched to comply with our research objectives and represents a comprehensive investigation of the knowledge sharing process (tacit knowledge sharing). Guiding framework also has been used by Siong and Salleh *et al.,* (2011) for KM implementation in a public sector organisation.

Guiding knowledge sharing framework connects KM enablers and the process to share the tacit knowledge in public-sector accounting organisation. It interconnects solutions of KM through culture, leadership, learning and technology to enhance knowledge sharing process in the organisation. Moreover, it enables the tacit knowledge sharing process and is useful as process of strategic KM which supports knowledge networks and knowledge flow for enhancing decision making process in the organisations. Figure 1 describes conceptual framework adopted to extend for knowledge transfer process to prevent ID theft in retail industry organisation.

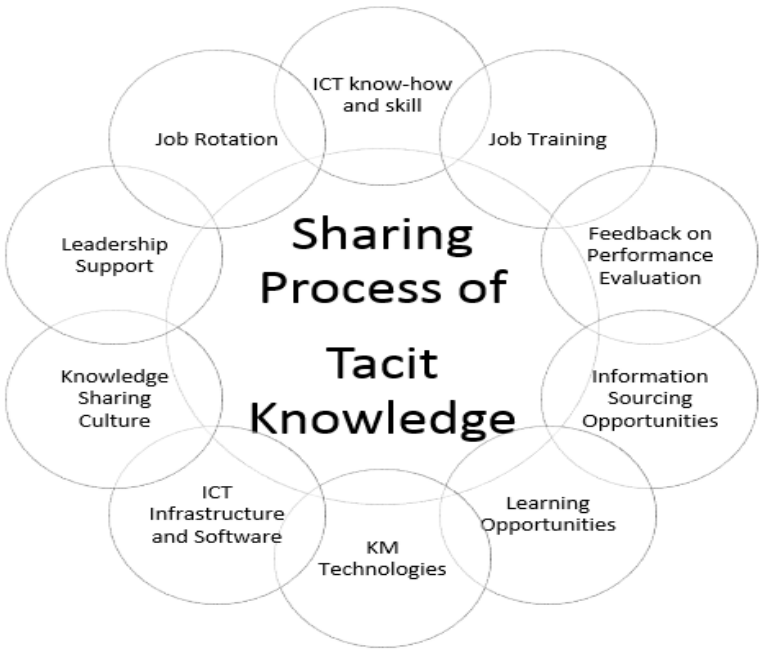

Figure 1: Conceptual Framework Proposed by Salleh (2010)

This framework has been adopted and extended within the context of improving knowledge transfer processes to prevent ID theft inside the organisation, as it supports to understand and manage various factors of this research, such as, information and communication technologies knowledge and skills of the individuals, information and communication technologies infrastructure and software, KM technologies available, job

training, rotation of jobs, feedback on the basis of performance evaluation, learning opportunities available, opportunities for sourcing information, support of leadership, culture of knowledge sharing (see Figure 1). It has been extended in the context of ID theft prevention knowledge sharing. Figure 2 describes the extended framework for knowledge transfer processes to prevent ID theft within retail industry organisation.

3. Methodology

Qualitative methods have been adopted by using a case study and focus mainly on the facts conveyed by a respondent. For example, what they do; through which the researchers are able to understand what is going on in a particular process or situation. These are efficient at illuminating issues and arriving at explanations such as an exploration of meaning (Gillham, 2000). In this approach, researchers seek to inspect issues related to the various operations of individuals or groups/teams of the personnel (Creswell, 2013). Therefore, interviews were conducted with individuals to determine how they personally experienced concerns over systems operations for ID theft prevention knowledge sharing.

A case study method with a set of procedures is required. These include design, collection of data, analysis of the data collected and reporting and presenting the results following the analysis of data collected during the case study research (Yin, 2011). Initially, a review of related literature to assess the extent of work previously completed in ID theft prevention was conducted and related questions for the data collection during the interviews in the organisation were designed. A pilot study was conducted with eight semi-structured interviews with PhD research students at the University of Central Lancashire, to test the research questions and the interview process for a real cases in a retail organisation.

Various approaches such as interviews, analysis of internal documents of selected organisations, including memos, survey reports of the organisation, their website, investigation of news in print and electronic media information about the organisation were used. Fourteen semi-structured interviews were conducted with individuals working in teams and groups inside the organisation from top management to support staff. Internal documents were examined to understand existing process of knowledge sharing to prevent ID theft. Several internal reports, memos and emails were studied to seek any evidence of ID theft, causes of stealing information of individuals and organisations and the steps taken to overcome these problems. Various news reports of the organisation published in print and digital media were also examined to discover evidence or clues about ID theft and its prevention.

The analysis method used included a combination of content analysis and a coding system. Contents analysis is a method used to determine the content of written, recorded and published communication through an objective, systematic and qualitative procedure. For the qualitative data analysis, the coding system followed the reflexive and recursive movement between development of concept, data-sampling and collection of the data, and interpretation and analysis (Bryman and Bell, 2011). The coding of data for analysis contained the cross-sectional design including data collected from relevant retail companies to establish the patterns. The NVivo software tool was used for content analysis and the coding system.

4. Case Study - Company A

A case study of this research project was completed. The company selected is the leading multi-brand retailer with approximately £2 billion annual sales, with multiple active customers receiving millions of products every year. Over three-quarters of the sales are processed online, one third of those being from mobile devices. About one million customers visit the website every day. Due to the privacy, further details of company are not provided. Fourteen semi-structured interviews and analysis of relevant company documents and literature were

completed. A confidentiality agreement was signed by researchers and the management before data collection. Interview participants were selected and consent was obtained through emails.

5. Findings

The various factors of the framework are shown in Figure 2. The questions were designed according to the framework extended (Figure 2) to fulfil the requirements of the research project. This section summarises the findings.

5.1. ICT Know-how and Training

Information and Communication Technology (ICT) refers to information communication by using telecommunication systems. ICT infrastructure plays a vital role in knowledge sharing among the individuals within and outside of the organisation. It is essential to understand ICT skills required to assess the ability of staff to use those skills to solve the complicated problems of information management, knowledge transfer and presentations (Cobo, 2013). These include learning and technological skills, such as developing ideas, sharing information and fact finding (Cobo, 2013; Dede, 2010). Employees required particular practical skills ('know-how') to perform required tasks efficiently. These can be learned and developed through independent learning or detecting and emulating the skills of others', which are the approaches of tacit knowledge sharing environment (Letmathe *et al.,* 2012). An advanced learning environment enables the workers to enhance their expertise to deal with complicated problems. Learning opportunities enhance progress by removing previous mistakes and weaknesses (Harteis *et al.,* 2008). Organisations provide various training opportunities for their employees to keep them up-to-date and to enhance the innovative techniques to improve performance.

The researcher asked various questions on training for knowledge sharing in the organisation and to investigate the effectiveness of the training provided to the workers to enhance the skills of ID theft prevention knowledge sharing and to determine opportunities for increasing. From the responses to the question "How do you get training to enhance your skills for knowledge sharing of ID theft prevention in your organisation?" interviewees explained that the training is provided for fraud prevention and to understand existing systems in the organisation. If a new system comes into the department then employees trained to operate that system and understand its functionalities (R1, R3, R12). When a new employee joins the company he/she gets induction training for 12 months to understand the existing systems and their role (R7).

Participant (11) responded that they had basic training to use and create spreadsheets in Excel and access the database at the start, but acquired knowledge from their own experience. They did not receive further training. He/she responded that:

"We've had Excel training, spreadsheets, Access database training, things that we'd need to produce our reports to the regional loss prevention managers. As for the fraud side of it, we haven't had a lot of training ourselves. It's basically self-taught."

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

Some participants stated that training to identify and prevent ID fraud is provided to the workers in the fraud prevention department only (R11, R13). While some responded that training is not being given to them at all (R11, R12). When asked for reasons why training was not being provided, some interviewees responded that they do not need training, as they are not working at the front end and they do not face customers directly. Participant (11) stated:

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

Another respondent (14) stated that these days fraudsters are smart and fast. ID fraudsters have adopted new techniques and methods to commit fraud and training doesn't help them to stop the fraud. This research found that at the moment the company provides other learning opportunities for the workers such as one-to-one meetings, the arrangement of seminars, and updates in meeting huddles regarding ID related fraud identification and prevention (R2). When asked about the advantages and usefulness of the learning opportunities, the participants responded that training could be advantageous (R1, R8, R10, R13).

When asked about the training provided for ID theft prevention knowledge sharing, all the responses were "No". Currently, the company does not arrange any training for sharing the knowledge of ID theft prevention. Participants even expressed the words:
"…we are not doing anything like that, we don't need training for sharing the knowledge of id theft prevention".

This investigation found that trainings and other learning opportunities can play vital role for enhancing the knowledge of employees for ID theft prevention. Participants responded for the requirements of learning environment for sharing the knowledge of ID theft prevention among staff members. Presently the company focuses on the prevention of personal information theft at customer level and they are not working on the development of enhanced knowledge transfer process the prevent ID theft within company. Therefore, it is recommended to develop system of ID theft prevention knowledge sharing among individuals and groups/ teams within company.

5.2. Information Sourcing Opportunities

Whilst enquiring about information sourcing opportunities, all respondents stated that information regarding ID theft issues and their solutions are being shared through email, policy documents and the internal network messaging system. For investigating the preferred method of sharing knowledge, the respondents stated that they prefer to use emails to receive information (R7, R8). Email as a knowledge sharing resource was used by the participants as emails provided most of the updated information regarding ID theft issues and their solutions. They were easier to use and easy to attach documents to send to the recipients. Furthermore, emails have quick access everywhere. Participant (11) responded:
"Email is quick and you can put whatever you like in it and attach documents and that's the main source we've always used."

According to participant (14), employees are being emailed to inform them of training available. The participant said that:
"Email is the best way, and I receive emails for availability of training."

When asked about the satisfaction of available sources, the researchers found that all participants were satisfied with the availability of knowledge sharing sources. For sources of sharing knowledge with staff of other departments, participants responded that they send and receive the required information through emails only.

Currently, the company uses the emailing system for disseminating information and there are some policy documents providing useful knowledge to the employees regarding the working environment and activities. They also have an internal messaging system called Yammer where employees post updates regarding their working activities (R1, R3, R10).

5.3. Job Rotation

Knowledge shared among individuals is concerned with establishing communication among workers inside the organisation. The most significant issue of knowledge sharing is the trust within the organisation; such as, how willing are people to share what they know?

Answering these questions leads us to activities based on trust building, team creation, job rotation and so forth (Sveiby, 2001).

Whilst investigating the job rotation process, it was found that within the company, jobs are not being rotated except via promotion from one job to another. According to interviewee (13):

"There isn't any job rotation," interviewee (10) responded: *"We don't do any rotation really with anybody else"*.

As discussed earlier, job rotation plays a vital role in increasing the knowledge of individuals and teams in the organisation, but in that company employees are learning from their own experiences. Participant (1) responded that a job is not being rotated from department to department to enhance the knowledge of ID theft prevention. Interviewees replied that their job could be moved from one seat to another seat if someone was not coming to work or someone was sick, so to fulfil that requirement of the work, employees are being moved to other seats (R1). If someone requires some information, he/she puts the question forward and obtains the knowledge for that question. Respondent (R3) said that:

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

Whilst asking the reason for not rotating jobs in the company, respondents said that they are all doing same job; the company doesn't need to rotate the jobs. Currently, the company does not rotate jobs to increase staff knowledge of prevention of ID theft and share their knowledge among others. It is strongly recommended that the company develops the job rotation process so that individuals and team members may enhance their knowledge and learn from the experiences of the workers moved from other working areas who have expertise via their work in ID theft prevention. The staff whose job has been rotated also increase their knowledge by working in a new environment.

5.4. Feedback on Performance Evaluation

Feedback is vital in the evaluation and monitoring of activities of employees. However, current developments in computerised technology are advancing the nature of monitoring the performance of employees (Alder and Ambrose, 2005). Feedback can be given for various purposes. These include bringing the resultant outcomes of the activities or the processes into focus; providing information when workers move away from primarily goals; helping to fix the new goals or adjusting the existing goals; and guidance to perform the activities. It also promotes critical reflection and brings about new approaches (Gabelica *et al.,* 2012). To investigate performance of employees, various questions were asked on feedback. Participant (1) said that:

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

Managers arrange monthly one-to-one meetings with the advisors to ask how things are going and how staff are performing their activities. Feedback is given to staff on the basis of their work and their level of success. The company also evaluates the performance of employees twice a year (R10).

Asking about tools being used for evaluating the performance of employees, respondents said that they have only one tool for evaluating the performance of employees and that is an e-learning system giving knowledge of evaluation modules (R8, R10, R13, R14).

Respondent (14) said that:

"It's an e-learning module. Each worker has to score a hundred per cent. If they don't, they have to re-sit it until they get a hundred per cent in both ID theft and ID fraud. But yeah, that is the only measurement in place."

For evaluating the performance of knowledge sharing with others, managers and advisors responded that the company is not evaluating performance on knowledge sharing of employees for ID theft prevention. Participant (10) said that:

"As for identity theft prevention and knowledge sharing, we're not evaluated on that."

Whilst asking about the impact of feedback, participants said that it is very important to evaluate the performance of working activities. By evaluating the performance of employees, their managers do have the knowledge that an employee is doing well and he/she has the knowledge of their working activities; they also know that staff are working as per the requirements and policies of the company. Furthermore, if they notice that someone requires some training or cannot work, then that employee should be trained or someone should help him/her in their working activities. The manager provided the feedback to staff in a one-to-one meeting or through email detailing how they are doing their work and what they need to increase and the need to go through re-training. The company needs to determine at what level employees learn about knowledge sharing regarding ID theft prevention and provide feedback to the workers.

5.5. Leadership Support

Leadership support is one of the most important element for enhancing the working environment of the organisation and encouraging staff towards achieving required goals. Various questions were asked for the investigation of requirement and availability of leadership support in the company. During investigation we found that management shares the information regarding ID theft issues through emails and monthly meetings. Participant (1) said:

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

Managers also arrange face-to-face meetings with workers (R2, R10). An internal network messaging system is also being used to share the knowledge to identify and counter issues. Additionally, management arranges seminars to update the workers' knowledge regarding ID theft and its prevention. Some participants from the fraud management and information security departments stated that they needed more technical manpower to prevent ID theft in the company. Asking about the support required, managers and staff were happy with the support of the leadership (R3). Some participants responded that they required quicker feedback. Interviewee (2) responded:

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

One of the participants reported that they required more staff as they cover whole the country (R10); he/she said:

"You can always do with more individuals to help because, you know, I mean for us, we cover the whole country. So more resources would be more manpower. "

The leadership of the company is very supportive to the workers and staff are happy with the facilities provided. Sometimes line managers walk down to the desks of the advisors and other employees to help them and to describe the activities performed in order to identify and counter ID fraud. During investigation we found that leadership of company is very supportive and helping. Employees are happy with them. When we talk about the ID theft prevention knowledge sharing, then gain there is the need of the enhanced environment for knowledge sharing to prevent ID theft. Support of management is required for development of that environment. So that staff and departments/teams can share knowledge each other to prevent ID theft within company.

5.6. Knowledge Sharing Culture

Knowledge sharing refers to the transfer of knowledge among individuals, different teams and departments inside the organisation and among different organisations (Section 2). Organisational culture refers to the shared values, beliefs and performances of persons within an organisation (McDermott and O'Dell, 2001). The knowledge sharing culture is the main elements considered for knowledge sharing among the individuals and teams within the organisation. It is the most important element that needs to be understood in advance before employing any new strategies in the organisation (Syed-Ikhsan and Rowland, 2004).

A knowledge sharing culture is considered to be a significant aspect since it controls the effects of other related variables such as existing technology and management techniques on the accomplishment of KM. According to Stoddart (2001), knowledge sharing can only work if the culture of the organisation supports it, and if the changes required are developed according to the culture of the organisation. In this regard various questions were asked about the knowledge sharing culture in the organisation. When asked about the trust of others, interviewees described that they trust other workers concerning knowledge sharing of ID theft prevention within their department, but they don't trust the people outside the department, such as the staff from other departments. Presently, knowledge is being shared only within departments of the company (R1, R12). Employees are not confident enough to share knowledge with the staff of other departments in order to prevent ID theft due to a lack of trust (R7). Therefore, individuals and teams are only getting the advantage of the expertise within their own department. The company needs to develop a system to educate the staff from different departments and raise awareness of ID theft and its prevention. They need to increase the level of trust within the organisation.

5.7. Knowledge Management Infrastructure

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

During the interviews, questions were asked to investigate the existing infrastructure including the software, hardware, networks and protocols developed for information security in the organisation and the skills required for knowledge sharing. More questions were asked about the availability of resources and to investigate the usefulness of the KM resources and any requirements for further resources. Whilst asking about the knowledge sharing tools being used for ID theft prevention, participants reported that various tools were being used for ID theft prevention, such as CIFAS, AQAFAX and KBA (R3), and it was found that for sharing the knowledge of ID theft prevention, the company has an e-learning system which provides information on training available to staff members; employees also upload their activities on the e-learning system. Respondent (1) said:

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

Furthermore, policy documents are being uploaded onto the intranet of the company and sometimes workers acquire the knowledge by using personal contacts. According to (R8):
"So it's a combination of both personal contact and also the intranet, written policies and written information which are available to all".

Whilst asking information technology skills required for ID theft prevention knowledge sharing, it was found that the basic skills are provided, such as how to use and create Excel spreadsheets and pilot tables (R11, R12). Some of the employees are trained to analyse the data through their own experience regarding ID fraud and encountering those frauds (R8). Although employees have a small level of skills, they all are very satisfied with the availability and usage of existing resources, having the skills from their own experience to work in the company and use the existing systems.

6. Discussion

This research included the process of research refinement by reviewing the existing literature and find out existing gape in the research area. By extensive review of the literature and comparing and contrast of existing frameworks, a knowledge sharing framework proposed by Salleh (2010) was adopted (Figure 1) for extension to enhance the knowledge transfer processes to prevent ID theft. Qualitative research methods were used to conduct case study in retail industry organisation. We designed the questions around factors of extended framework (Figure 2) of this research to fulfil the requirements of the research project. Conducted a pilot study having eight interviews with research students at University of Central Lancashire, UK. A real world case study was conducted from a well reputed online retailer in UK. Data collection included fourteen one-to-one semi-structured interviews with staff members of various departments of the company, news investigation of print and electronic media and document analysis of the company including website of the company.

As discussed earlier, in this paper we extended the conceptual framework proposed by Salleh (2010) in the context of knowledge transfer process to prevent ID theft in retail industry organisation (Figure 2). Furthermore, the important and relevant factors in the adopted framework (Figure 1): job rotation, feedback on performance evaluation, information sourcing opportunities, leadership support, and knowledge sharing culture are included for ID theft prevention knowledge transfer in the extended framework (Figure 2). Moreover, the factor ICT know-how and trainings has been produced (in extended framework) from the merger of three factors ICT know-how and skills, job training and learning opportunities in adopted framework. Those three factors could be used for the same purpose, such as, job training are learning opportunities for ICT know-how and enhancing skills for ID theft prevention knowledge sharing in the organisation (Table 2). The factor knowledge management infrastructure has been produced from ICT infrastructure and software and knowledge management technologies factors of the adopted framework as knowledge management infrastructure (in extended framework) used for ID theft prevention knowledge transfer includes the hardware, software protocols and techniques. Therefore, the two factors were also merged to form another factor as per requirements of this research (Table 2).

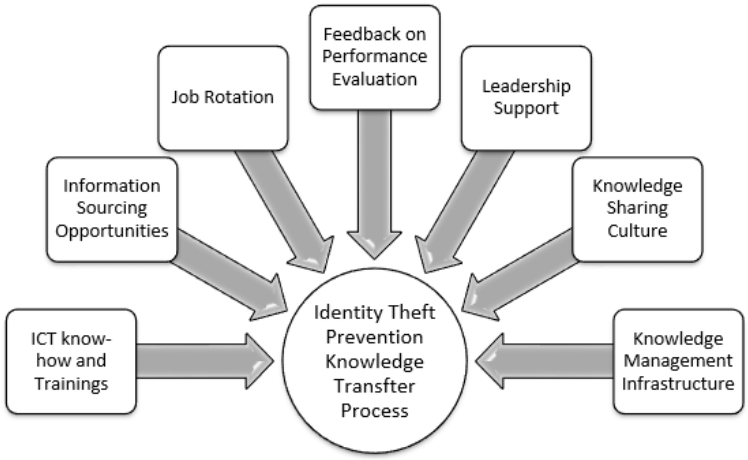

Figure 2: Extended Framework for Knowledge Transfer Process to Prevent Identity Theft in Organisation

Figure 2 presents the extended framework for the knowledge transfer process of ID theft prevention. It has seven factors: information and communication technology; information sourcing opportunities; job rotation; feedback on performance evaluation; leadership support; a knowledge sharing culture and a knowledge management infrastructure. Table 2 describe the extended framework from guiding framework proposed by Salleh (2010).

	Salleh (2010) Framework	Extended Framework for Knowledge Transfer Process to Prevent Identity theft
Context	- Knowledge sharing framework connects knowledge management holders and tacit knowledge sharing process in public sector accounting organisation.	- Enhances the knowledge transfer process for ID theft prevention in retail organisation.
Revised Factors Extended	- Contains the factors ICT know-how and skill, Job Training, Job Rotation, Feedback on Performance Evaluation, Learning Opportunities, Information Sourcing Opportunities, Leadership Support, Knowledge Sharing Culture, ICT Infrastructure and Software and KM Technologies.	- Factors Information Sourcing Opportunities, Job Rotation, Feedback on Performance Evaluation, Leadership Support and Knowledge Sharing Culture are adopted from guiding framework. - The factor ICT know-how and trainings has been produced from the ICT know-how and skills, job training and learning opportunities in adopted framework. - Knowledge management infrastructure has been produced from ICT infrastructure and software and KM technologies in adopted framework.
Contribution	- Integrates KM solution by leadership, learning, technology and culture for enhancing the knowledge sharing process in public sector organisation.	- Helps the retail industry to enhance the process of knowledge sharing for ID theft prevention in organisation. - Provides solutions for developing knowledge sharing culture in company. - Enable the organisation for development appropriate training system to educate the staff to share knowledge of ID theft prevention.

Table 2: Comparison of Extended and Existing Framework

During the investigation we found that, currently the company provides induction training to newcomers on the existing systems and working activities at a basic level such as spreadsheets and fraud databases (Table 3). An e-learning system is being used to upload the information for available training. Educational seminars are arranged. However, the company does not have a training system for ID theft prevention knowledge sharing.

An advanced learning environment enables the workforce to deal with the complex problems faced. The company still needs to enable the staff of all departments to receive training regarding ID theft prevention practice and prevention. Table 3 summarises strengths

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

Table 3: Summary Table for Strengths, Weaknesses and Recommendations

and weaknesses for knowledge sharing of ID theft prevention and recommendations by the investigation of this research.

The emailing system is used for information transfer amongst the staff; sometimes an internal networking system is being used called Yammer for updating the employees regarding ID theft issues. At the moment, the company uses CIFAS and AQAFAX as knowledge sharing

tools for ID theft prevention. The company needs to enhance the knowledge sharing culture for ID theft prevention; at the moment individuals are sharing their knowledge with each other within a department and they trust those who are working with them within that department. Therefore, staff of other departments are not getting the advantage of ID theft prevention knowledge sharing. As a result, also recommended is the development of a system for ID theft prevention knowledge sharing and the education of the workers in the process of knowledge sharing.

7. Conclusions

Findings of this study illustrate that knowledge of ID theft prevention is not being shared among individuals and between teams across the departments. Staff share knowledge of ID theft prevention within their own departments. Basic training is being given to newcomers to provide them with the know-how about the systems used and working activities within the company.

Seminars are arranged on ID theft prevention. The company needs to develop an educational system to enhance the knowledge of employees in ID theft prevention knowledge sharing. Some policy documents are being disseminated to employees on ID theft prevention which set out awareness of confidential information but those documents do not describe knowledge sharing for ID theft prevention. E-mails are used to share their knowledge for their working activities. The company needs to develop a centralised system that can provide information to the employees in ID theft prevention.

There is no job rotation in the company and employees are learning from their own experience which is time consuming and exhaustive. The importance of job rotation in the organisation to enhance the knowledge of individuals, teams and groups. Company needs to rotate the knowledge holders' jobs around different teams/groups in varying departments to enhance knowledge of other staff members of ID theft prevention. Employees trust others within their department and share knowledge with them regarding preventing ID theft. The company needs to enhance the trust level across departments for ID theft prevention knowledge sharing.

This research may help the retail industry enhance the process of knowledge sharing to prevent ID theft within the organisation and provide solutions on developing a knowledge sharing culture inside the company. It may also help the organisation to develop a proper training system to educate the staff to share their knowledge of ID theft prevention. This research also extends a framework in terms of ID theft prevention and sharing knowledge of ID theft prevention. Only one case study in retail industry organisation in the UK was used. Further case studies need to be conducted in different organisations and other countries and a cross-comparison would be useful to check the applicability of extended framework.

References

Aimeur, E. and D. Schonfeld (2011), "The ultimate invasion of privacy: Identity theft", *9th Annual International Conference on Privacy, Security and Trust 2011*, IEEE, Montreal, QC, pp. 24-31.

Alder, G.S. and Ambrose, M.L. (2005), "An examination of the effect of computerized performance monitoring feedback on monitoring fairness, performance, and satisfaction", *Organizational behaviour and human decision processes*, Vol. 97, No. 2, pp. 161-177.

Amin, A., Hassan, M.F.B. and Ariffin, M.B.M. (2010). "Framework of intrinsic and extrinsic motivators of knowledge sharing: A case of training institutes of an oil and gas company in Malaysia", *Information Technology International Symposium2010*, IEEE, Vol.3, pp. 1428-1432.

Arachchilage, N.A.G., Love, S. and Scott, M. (2012), "Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding Phishing Attacks", *International Journal for e-Learning Security*, Vol. 2, No. 2, pp. 127-132.

Bilge, L., Strufe, T., Balzarotti, D. and Kirda, E. (2009). "All your contacts belong to us: automated identity theft attacks on social networks", *18th international conference on World wide web 2009*, ACM, New York, pp. 551-560.

Bindra, G.S., Shrivastava, D. and Seth, R. (2012), "With attackers wearing many hats, prevent your "Identity Theft", *6th International Conference on Application of Information and Communication Technologies 2012*, IEEE, Tbilisi, pp. 1-5.

Bose, I. and Leung, A.C.M. 2013, "The impact of adoption of identity theft countermeasures on firm value", *Decision Support Systems*, Vol. 55, No. 3, pp. 753-763.

Bradford, T. and Cundiff, B., (2006). "Payments fraud: consumer considerations, Payments System Research Briefing", *Federal Reserve Bank of Kansas City*, 2006, Avialable at: https://www.kansascityfed.org/PUBLICAT/PSR/Briefings/PSR-BriefingMay06.pdf (accessed 07 December 2015).

Bryman, A. and Bell, E. (2011), *Business Research Methods 3e*, Oxford university press.

CIFAS (2012). "FRAUDSCAPE Depicting the UK's fraud landscape", Available at:
https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External%20-%2000%20Fraudscape%202012.pdf (accessed 10 June 2012).

CIFAS (2013). "FRAUDSCAPE Depicting the UK's fraud landscape" Available at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External-Fraudscape_2013_CIFAS.pdf (accessed 10 July 2013).

Clough, J. (2015), "Towards a common identity? The harmonisation of identity theft lawsnull", *Journal of Financial Crime*, Vol. 22, No. 4, pp. 492-512.

Cobo, C. (2013), "Skills for innovation: envisioning an education that prepares for the changing world", *Curriculum Journal*, Vol. 24, No. 1, pp. 67-85.

Conrad, E., Misenar, S. and Feldman, J. (2012), *CISSP study guide*, Elsevier.

Creswell, J.W. (2013), *Research design: Qualitative, quantitative, and mixed methods approaches*, Sage Publications, Incorporated.

Dede, C. (2010). Comparing frameworks for 21st century skills. In J. Bellance, & R. Brandt (Eds.), *21st century skills: Rethinking how students learn?* Solution Tree Press, Bloomington, pp. 51-76.

Fennelly, L.J. (2012), *Handbook of loss prevention and crime prevention*, Access Online via Elsevier.

Fire, M., Goldschmidt, R. and Elovici, Y. (2013). "Online Social Networks: Threats and Solutions Survey", *Communications Surveys & Tutorials*, IEEE, Vol. 16, No. 4, pp. 2019 – 2036.

Gabelica, C., Bossche, P.V.d., Segers, M. and Gijselaers, W. (2012), "Feedback, a powerful lever in teams: A review", *Educational Research Review*, Vol. 7, No. 2, pp. 123-144.

Gillham, B. (2000), *Case study research methods*, Continuum International Publishing Group, London.

Grover, A., Berghel, H. and Cobb, D. 2011, "The State of the Art in Identity Theft" in *Advances in Computers*, ed. Marvin V. Zelkowitz, pp. 1-50.

Guang-bin, C., Liang, D., Yi-Jun, L. and Tao, G. (2010), "Study on Multi-levels Incentive Mechanism Model for Tacit Knowledge Sharing in Enterprise", *International Conference on E-Business and E-Government 2010*, IEEE , Guangzhou, pp. 1948 - 1951.

Harteis, C., Bauer, J. and Gruber, H. (2008), "The culture of learning from mistakes: How employees handle mistakes in everyday work", *International Journal of Educational Research*, Vol. 47, No. 4, pp. 223-231.

Israilidis, J., Siachou, E., Cooke, L. and Lock, R. (2015), "Individual variables with an impact on knowledge sharing: the critical role of employees' ignorancenull", *Journal of Knowledge Management*, Vol. 19, No. 6, pp. 1109-1123.

Jin, L., Takabi, H. and Joshi, J.B. (2011), "Towards active detection of identity clone attacks on online social networks", *first ACM conference on Data and application security and privacy 2011*, ACM, New York, pp. 27-38.

Lai, F., Li, D. and Hsieh, C.T. (2012), "Fighting identity theft: The coping perspective", *Decision Support Systems*, Vol. 52, No. 2, pp. 353-363.

Letmathe, P., Schweitzer, M. and Zielinski, M. (2012), "How to learn new tasks: Shop floor performance effects of knowledge transfer and performance feedback", *Journal of Operations Management*, Vol. 30, No. 3, pp. 221-236.

Li, P.T. and Kuan, Y.W. (2015), "Linkage between knowledge management and manufacturing performance: a structural equation modeling approachnull", *Journal of Knowledge Management*, Vol. 19, No. 4, pp. 814-835.

McDermott, R. and O'Dell, C. (2001), "Overcoming cultural barriers to sharing knowledge", *Journal of knowledge management*, Vol. 5, No. 1, pp. 76-85.

Musulin, J., Gamulin, J. and Crnojevac, I.H. (2011), "Knowledge management in tourism: The importance of tacit knowledge and the problem of its elicitation and sharing", *MIPRO, Proceedings of the 34th International Convention 2011*, IEEE, Opatija, pp. 981 - 987.

Noor, N.M. and Salim, J. (2012). "The influence of individual, organizational and technological factors on knowledge sharing in the private sector in Malaysia", *International Conference on Information Retrieval & Knowledge Management 2012*, IEEE, pp. 167-171.

Reyns, B.W. (2013), "Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses", *Journal of Research in Crime and Delinquency*, Vol. 50, No. 2, pp. 216-238.

Romanosky, S., Telang, R. and Acquisti, A. (2011), "Do data breach disclosure laws reduce identity theft?", *Journal of Policy Analysis and Management*, Vol. 30, No. 2, pp. 256-286.

Sakharova, I. (2012), "Payment card fraud: Challenges and solutions", *International Conference on Intelligence and Security Informatics 2012*, IEEE, Washington, D.C, pp 227 - 234.

Salleh, K. (2010), "Tacit Knowledge and Accountants: Knowledge Sharing Model", 2nd International Conference on Computer Engineering and Applications *2010*, IEEE, Bali Island, pp. 393.

Shaobo Ji, Jianquan Wang, Qingfei Min and Smith-Chao, S. (2007), "Systems Plan for Combating Identity Theft - A Theoretical Framework", *International Conference on Wireless Communications, Networking and Mobile Computing, WiCom 2007*, IEEE, Shanghai, pp. 6402.

Siong, C.C., Salleh, K., Syed Noh, S.A. and Syed-Ikhsan Syed, O.S., (2011). KM implementation in a public sector accounting organization: an empirical investigationnull. *Journal of Knowledge Management*, Vol., No. 3, pp. 497-512.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: A literature review", *International Journal of Information Management*, Vol. 36, No. 2, pp. 215-225.

Stephen Harrison., (2013). "Annual Fraud Indicator, March 2012. National Fraud Authority". Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf.

Stoddart, L. (2001), "Managing intranets to encourage knowledge sharing: opportunities and constraints", *Online information review*, Vol. 25, No. 1, pp. 19-29.

Sveiby, K. (2001), "A knowledge-based theory of the firm to guide in strategy formulation", *Journal of intellectual capital*, Vol. 2, No. 4, pp. 344-358.

Syed-Ikhsan, S.O.S. and Rowland, F. (2004), "Knowledge management in a public organization: a study on the relationship between organizational elements and the performance of knowledge transfer", *Journal of knowledge management*, Vol. 8, No. 2, pp. 95-111.

Trkman, P. and Desouza, K.C. (2012). "Knowledge risks in organizational networks: An exploratory framework", *The Journal of Strategic Information Systems*, Vol. 21, No. 1, pp. 1-17.

Wenjie Wang, Yufei Yuan and Archer, N. (2006). 'A contextual framework for combating identity theft', *IEEE Security & Privacy*, Vol. 4, No. 2, pp. 30-38.

Yan Li and Zetian Fu. (2007), "A Framework of Knowledge Transfer Process in Expert System Development", *International Conference on Wireless Communications, Networking and Mobile Computing 2007*, IEEE, Shanghai, pp. 5597-5600.

Yin, R.K. 2011, Applications of case study research, London, Sage.