The Prevention of Internal Identity Theft-Related Crimes: A Case Study Research of the UK Online Retail Companies

by

Romanus Izuchukwu Okeke

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

May 2015

STUDENT DECLARATION

Concurrent registration for two or more academic awards

I declare that while registered as a candidate for the research degree, I have not been 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 PhD

School Lancashire Business School

ABSTRACT

Ranked the third biggest cyber security threats of 2013 by Forbes, Internal Identity Theft-Related Crimes (IIDTRC) leave countless victims in their wake, including online retail companies and consumers. With the rapid growth in the use of credit and debit cards in e-commerce, the online retail has been a key target for the IIDTRC perpetrators. IIDTRC involve the misuse of information systems (IS) by the dishonest employees to steal victims' personal identifiable data. The crimes pose significant socio-economic impact and data security risks. In the context of online retail, relatively little research has been done to prevent IIDTRC. A few studies focus on situational-based IIDTRC prevention approach built on an independent use of software security. Others develop IIDTRC prevention frameworks in the context of generic e-businesses. The majority of the frameworks have little or no grounded empirical research. This research entitled the 'The Prevention of Internal Identity Theft Related Crimes: A Case Study Research of the UK Online Retail Companies', attempts to bridge this research gap. It provides answers to two questions – what is the nature of IIDTRC in online retail companies and what framework can be used for IIDTRC prevention.

This research set out three aims to answer the two questions. First, it provides understanding of causes, methods of carrying out and prevention of IIDTRC. Second, it extends a role-based framework (RBF) for the prevention of IIDTRC. Third, it evaluates the extent the RBF can be applied in the prevention of IIDTRC in online retail companies. A qualitative case study was used to achieve these aims. The empirical data were collected in the northwest of UK from 2011 to 2013. The field study was carried through archival analysis, semi-structured interview and participant observation. Organisational role theory (ORT) was used to guide the concept of a role-based framework (RBF) – a collaborative approach where the key components of management work in unison is required to prevent IIDTRC. The attributes of RBF were synthesised from the recommended IIDTRC prevention practices.

The empirical evidence suggests that IIDTRC perpetrators in online retail companies are likely to be the top management and call centre employees. The findings suggest that online retail consumers' credits/debits cards details are as much vulnerable to IIDTRC as the companies' identities such as trade secrets and trademarks. Furthermore, the common methods used by the IIDTRC perpetrators include collaboration, collusion, infiltration and social engineering.

Some of the IIDTRC prevention practices, of which the majority is software security, are implemented without considering the contribution of human-centred security based on management roles. In examining the contribution of the management roles in implementing Information Systems security practices, major challenges that are faced by online retail companies were identified. They include lack of resources, lack of management support and lack of IIDTRC prevention awareness training.

This research concludes that an application of RBF can reduce the impact of the identified challenges. This was suggested by applying RBF in conducting IS security auditing in three online retail companies. The finding from the selected companies suggests that the RBF approach can maximise management performance in providing effective IIDTRC prevention practices. It provides better returns on cost, quality and time in the IS security auditing. It has an impact on management attitudes on preventing IIDTRC by clarifying and aligning their roles in implementing effective IS security auditing. There is heterogeneity of this effect across the companies suggesting that some are utilising the RBF approach while others are not. The finding confirms the plausibility of the RBF attributes. It suggests that the human-centred security play an integral role for effective internal data security in preventing IIDTRC. It suggests that it pays to use the collaborative management roles approach for implementing IIDTRC prevention practices. Furthermore, the use of the RBF approach can improve the effectiveness of the online retail companies in preventing IIDTRC.

The findings suggest that benefits may accrue from the RBF approach when supplemented with a collaborative IS auditing. The benefits depend on the level of management IT skills, their perception of their roles, top management support and the organisational operations. This research contributes to the literature in identity theft prevention in online retail. To IS security practitioners, it identifies the data security challenges and IIDTRC prevention practices. To theory, it extends a role-based framework for IIDTRC prevention. To the emerging research in the digital economy, it puts forward as a robust starting point for further related works in cyber security, cybercrimes prevention and criminology.

TABLE OF CONTENTS

CHAPTER 2

LITERATURE REVIEW

CHAPTER 4

RESEARCH PHILOSOPHY AND METHODOLOGY

CHAPTER 5

DATA COLLECTION

CHAPTER 6

DATA ANALYSIS AND RESULTS

CHAPTER 7

RESEARCH DISCUSSION

CHAPTER 8

CONCLUSION

LIST OF FIGURES

LIST OF TABLES

List of Tables Continued

ACKNOWLEDGEMENTS

Thanks to God Almighty for helping me throughout this research endeavour. To my loving wife Mrs Favour Makuochukwu Orji-Okeke and my wonderful elder brother, Mr Sabastine Nwachukwu, you both have been my inspiration. You are my constant source of encouragement, many reasons to smile and the joy that knows no bounds and greatly deserves my appreciation and deepest gratitude. To my late mum and dad: Mr and Mrs Job Nwachukwu DimOkeke, who have slept in the Lord. Dad and Mum, I wish you were here to witness the completion of this research, but I know you are resting in the bosom of the Lord, rest in peace. You both are greatly missed, but you are always in my thoughts. To my sisters – Mrs Chima Oguji, Mrs Sabina Obiora and my mother-in-law – Mrs Philomina Orji and my brothers-in-law – Onyeabo Oji and Azuka Oji, and my nephews and nieces; thank you all for your prayers and encouraging me throughout my period of study. We have gone through this research together. I am the best man; husband, brother; in-law and uncle that I can be because of your support. I am proud of you all and I love you beyond words.

Second, my appreciation goes to my director of studies, Dr Mahmood Shah, and my supervisors, Dr M. Schulze, Prof. Y. Yusuf and Prof. T. Arum. Thanks to lecturers at Lancashire Business School – Dr M. J. Larson (my Research Degree Tutor), - Dr. P. Thomas (my PGCE Research Tutor) and Dr M. Meckel (my Referee); you have been supportive throughout my research; and key administrative staffers in the UCLan's Research Student Registry, M. Fisher, C. Altham and C. Wiggans for their support. Staffers of the School of Computing, Engineering and Physical Sciences, UCLan have been source of motivation over the years, particularly Prof. J. C. Read and Dr. P. Gregory of whose Information Systems research coaching got me started in the right direction. Thanks to fellow PhD candidates B. Izidor, C. Ibeachu, Barrister I Onyesi, R. Eben, O. Friday, C. Amasiatu and A. Usman who could always be relied upon for conversation, drink and coffee, and sharing most moments of my non-academic life, and nourishing my ambitions and hopes with their *joie de vivre.*

Finally, thanks to all the participants in this research for their support. I also acknowledge the financial support of the *ShopDirectGroup* and the Security and Information Systems Research Group of the Institute for Security and Information Systems Research (ISISR), Lancashire Business School; none of these organisations is identified with the contents, opinions expressed and conclusions of this research.

LIST OF ACRONYMS AND MEANINGS

ABCP	Association of Business Crime Partnerships
ACFE	Association of Certified Fraud Examiners
ACPO	Association of Chief Police Officer
ACPR	Australasian Centre for Policing Research
APWG	Anti-Phishing Working Group
APWG	Anti-Phishing Working Group
ATM	Automated Teller Machine
BRC	British Retail Consortium
BSBS	Basel Committee on Banking Supervision
CCA	Consortium for Cyber-security Action
CCTV	Closed circuit television
CIFAS	Credit Industry Fraud Avoidance System
CRSA	Control Risk Self-Assessment
DBIR	Data Breach Investigation Report
DFRWS	Digital Forensics Research Workshop
DHCP	Dynamic Host Configuration Protocol
DPA	Data Protection Act
e-Business	Electronic Business
EISIC	Intelligence and Security Informatics Conference
EMET	Enhanced Mitigation Experience Toolkit
e-Tailing	electronic retailing

List of Acronyms and Meanings Continued

FCSA	Financial Crime and Service Authority
FSS	Forrester and Seeburger Security Services
FTC	Federal Trade Commission
GIA_DSE	Global Information Assurance and Data Security Essentials
GIAC- GSEC	Global Information Assurance and Security Essentials Certification
HTTP	Hypertext Transfer Protocol
I.T	Information Technology
ID Theft	Identity Theft
IDTheft ADA	Identity Theft and Assumption Deterrence Act
IDTRC	Identity Theft Related Crimes
IIDTRC	Internal Identity Theft Related Crimes
IP	Internet Protocol
ISA	Information Systems Security Audit
ISACA	Information Systems Audit and Control Association
ISBS	Information security Breaches Survey
ISO	International Organisation for Standardisation
ITRC	Identity Theft Resource Centre
MIS	Management Information System
MPS_OS	Metropolitan Police Operation Sterling
NFA	National Fraud Authority
OCSR	Organised Crime Strategy Report
OECD	Organisation of Economic Cooperation and Development

List of Acronyms and Meanings Continued

PCeU	Police Central e-Crime Unit
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PID/I	Personal Identifiable Information/Data
QPS_MFIG	Queensland Police Service Police Major Fraud Investigative Group
RBF	Role-Based Framework
SOCA	Serious Organised Crime Agency
SSH	Secure Shell
U.K	United Kingdom
U.S	United States
UK ACAS	United Kingdom Advisory, Conciliation and Arbitration
UK AFI	United Kingdom Annual Fraud Indicator
UK CSS	United Kingdom Cyber Security Strategy
UK NAO	United Kingdom National Audit Office
UK ONS	United Kingdom Office for National Statistics (ONS),
UK_CDA	United Kingdom Crime and Disorder Act
UK_FAP	United Kingdom Fraud Advisory Panel
UK_HOCPU	United Kingdom Home Office Crime Prevention Unit
UK_NSDR	United Kingdom National Staff Dismissal Register
UNCPCJ	United Nations Congress on Crime Prevention and Criminal Justice
US DARPA	United States Defence Advanced Research Projects Agency
US NICCP	United States National Infrastructure Cyber Crime program

CHAPTER 1

RESEARCH INTRODUCTION

This chapter provides the background of this research. It introduces research aim and objectives, research questions, research methodology, research benefits, and outline of the thesis.

1.1 Research Background

Ranked the third biggest cyber security threats of 2013 by Forbes, Internal Identity Theft Related Crime (IIDTRC) leaves countless victims in their wake, including online retail companies and consumers (Fraud Watch, 2013). The widespread use of credit and debit cards through information systems (IS) has led to rapid growth in the online retail. This increasing mode of online retail operation has left consumers vulnerable to identity theft related crimes. It has been a general belief that the external criminals such as hackers and their collaborators perpetrate IIDTRC.

Several studies (e.g. Collins, 2006; Jamieson *et al.*, 2008; Fraud Watch, 2013) suggest that dishonest employees perpetrate the majority of cases of identity theft related crimes. IIDTRC involve unlawful manipulation' of IS as well as human beings by the dishonest or disgruntled employees to steal business/customers' identity to commit criminal offences (OECD[1], 2013). IIDTRC perpetrators carry out 'internal' identity theft related crimes (IIDTRC) by exploiting the data security loopholes and accidental data leakages.

Internal identity theft related crimes pose considerable socio-economic impact and data security risks to online retail companies, which in turn imposes responsibility on the data security management and IS researchers (CIFAS, 2013). The Ponemon Institute's DarkReading, which was cited by Widup (2010), suggests that malicious insiders: internal identity theft related criminals are the most common types of attacks among web-borne attacks and malicious code. DarkReading suggests malicious insiders make more than 90 per cent of all cybercrime costs per organisation every year.

[1] Organisation for Economic Co-operation and Development

1.2 Internal Identity Theft Related Crimes: Extent of the Problem

The evolution of e-businesses has left their customers vulnerable to internal identity theft related crimes (IIDTRC), which leave countless victims in their wake, including online retail companies. In 1990s, when the first third party services – First Virtual, Cybercash, and Verisign for e-businesses transactions were introduced, Greenberg and Barling (1996) noted that about 62 per cent of employees perpetrated IIDTRC in e-businesses. Recent studies hold that IIDTRC is on the rise (Skolov, 2005), and that significant figure of as much as 70 per cent of IIDTRC are committed in the workplace (Collins, 2006). CIFAS (2013) suggests that the socio-economic costs of internal identity theft crimes to e-businesses are inestimable. Due to increasing incidents of internal identity theft related crimes across world regions and business sectors, it is arguably difficult to record actual socio-economic costs. The costs range from irreparable brand and psychological damage to the victims to name but a few.

1.3 Internal Identity Theft Related Crimes: Global Issue

The incidents of internal identity theft related crimes (IIDTRC) in businesses across the world have not decreased for the past decades. KPMG, Kroll and CIFAS Joint Survey suggest that employees' fraud and IIDTRC related losses cost more than $1.4 million per one billion US dollars of sales (Kroll Global Fraud Report, 2013). This survey indicates that information theft and internal financial fraud are top rated irrespective of the world regions, except in Pacific East where the intellectual property (IP) counterfeiting and collusion are of high percentages. This is in line with the Association of Certified Fraud Examiners (ACFE) suggestions cited in Wells (2010) which suggests that majority of businesses lost 5 per cent of its annual revenue to IIDTRC – which account to more than 80 per cent of 1, 900 cases of employee's fraud. Identity Theft Resource Centre (2008) reports that IIDTRC cost businesses across the world about $221 billion annually; with businesses in the UK and USA over £3.2 billion and $50billion respectively per annum.

In Canada, identity theft is rated fastest growing among other crimes. In Australia, the cost is estimated to be more than $3 billion of which businesses losses accounted for between AUD$1 billion and AUD$4 billion (Queensland Police Service Police (QPS) Major Fraud Investigative Group, 2009). The Queensland Audit Office attributed this cost to the muddled attitude of the most top business managers who generally believe that identity theft related crimes are principally carried out online by hackers and their collaborators (Prosch, 2009; Passmore, 2009; Walliker, 2006).

In contrast to the Australian case of IIDTRC, the Organised Crime Strategy Report (OCSR) (2005-2009) suggests that more than 80 per cent of the senior executives admitted that they have been hit by the IIDTRC. From this OCSR's survey, IIDTRC accounted for the record loss by surpassing any kind of staff frauds for the first time in four year of OCSR's survey history. This report further notes that 48 per cent of these top business executives agreed that risks of IIDTRC dissuaded their contemporary e-business entries across the world. Potter and Waterfall (2012) suggest that many institutions and business leaders have spent more than £38 billion as part of global cyber security strategies for the prevention of IIDTRC. Identity Theft Resource Centre (ITRC) (2008) noted that lack of reliable data on the cases of IIDTRC has been one of the major challenges of preventing of IIDTRC and may continue to inhibit research into possible intervention strategies.

ITRC's Identity Theft: The Aftermath (2005-2008) has consistently argued that business stakeholders in some cases declined to report internal thefts to law enforcement since they are deemed to protect the name of their organisation. This argument was supported by Dean *et al.*, (2012) in their interview of 850 senior-level executives to examine the impact of IIDTRC on their companies' brand names. Dean *et al*., (2012) found that with business brands that worth between $1 million to $10 billion the average minimum loss associated with IIDTRC was 12 per cent of their brand value. This report supports the argument of ITRC (2008) in relation to the reason some business managers refuse to admit the scale of the IIDTRC problems. They tend to protect their jobs and the business brands names from the potential reputational damage. IBM Research agrees to this argument of business managers protecting their reputation and reported that 73 per cent of IS employees fears losing their job in the incident of IIDTRC (Chen and Rohatgi, 2008).

1.3.1 Internal Identity Theft Related Crimes: UK Issue

The UK National Audit Office Report (2013) on cyber security strategy suggests that cybercrime costs more than £27 billion per annum with the majority of this cost (£21billion) attributes to IIDTRC from UK businesses. National Fraud Authority (NFA) Report (2013) which uses systematic research techniques to analyse employee's related fraud has estimated that fraud loss against the UK business to be more than £73 billion per annum. In this report, identity theft related crimes accounted for 14.1 per cent while 31.3 per cent of this loss is associated with the IIDTRC.

Based on the UK's Staff Fraudscape by Hurst (2010) which estimated the cost of IIDTRC in UK businesses to be £3.2 billion, it can be arguably concluded that the cost of IIDTRC to UK businesses has increased by 7 folds since 2010.In as much as the costs for IIDTRC are on the rise so are the numbers of victims. Kroll Global Fraud Report (2013) indicates that 48 per cent of businesses in the UK are victims of IIDTRC. This report agrees with the CIFAS: Fraud Prevention Fraud Service (2012) that the UK is second to Iceland with highest incidents of the IIDTRC amongst 25 nations, which in turn supports Hub International's (2010) report that IIDTRC have has become one of the fastest growing employee's fraud in the UK. CIFAS (2012) indicates that there is more 50 per cent rise in the number of cases of IIDTRC compared to the previous years; which account for as much as 80 per cent of all computer and internet related crimes.

In support of with CIFAS (2012), Dean *et al.,* (2012) note that IIDTRC increase approximately by 30 per cent from 2011 to 2012. CSO Magazine (2011) also indicated that IIDTRC cases have increased from 55 per cent to 60 in every year period since 2008. Romanosky, Telang, and Acquisti (2008) reported that in the 217 cases of IDTRC in the companies they investigated of which 53 per cent of the sources of their losses could be determined, 26.5 per cent of these cases originated from the companies.

1.3.2 IIDTRC: Case of UK Online Retail Companies

It is not an uncommon to report for a continuous rise in the cost of the IIDTRC in UK online retail sector. As cited in the previous section, Kroll Global Fraud Report (2013) placed the UK online retail as one of e-business sectors where the incidents of IIDTRC are prevalent. In line with the Kroll's (2013) report, the British Retail Consortium (BRC) (2013) survey indicates that retail frauds have increased with the identity theft related crimes on the rise. This survey also suggests that one in three consumers do not shop from online because of perceived online retail information security loopholes. This suggestion agrees with Shah, Okeke and Ahmed (2013) that issues of privacy related to security concerns are a major challenge for the UK retail companies to tackle. The trend in the increasing cost of IIDTRC has not decreased for a decade in UK retail sector. In 2004, the estimated cost of IIDTRC to UK retailers was estimated to £498 million which was doubled to £282 million with respect to the 2003 report (CIFAS: Staff Fraud Report, 2012); which outweighs other business sectors in comparison.

The above reports support Stickley's (2009) suggestion that the incidents of IIDTRC is considerably more in online retail than in other business sectors due to modes of its business operation. In contrast to the cause of rising incidents of IIDTRC that has been linked to retail business operation by Stickley (2009), the CIFAS Fraud Report (2011) note that 76 per cent of retailers agreed that the increase of the IIDTRC incidents might be linked to recent economic crises. This report revealed that there is an increase of 19.86 per cent of identity theft related fraud cases in 2010 compared with the figures from the first quarter of 2009. This report suggests that more than 70 per cent of internal identity theft related crimes accounted for the total identity fraud committed. This report also corresponds to Gill's (2011) suggestions that there are tendencies of employees engaging in IIDTRC due current global adverse economic climate.

The impacts of IIDTRC losses and damage are inestimable. In some cases, businesses were unable to recover the cost of the damage, especially smaller businesses like online retailing where these crimes discourage emerging smaller retailers from going into e-commerce (Yuan, 2005). Other impacts reported by Kroll (2013) include outraged customers, soured B2B relationships, decrease in corporate earnings, loss of investor's confidence, job losses, and legal settlements, psychological issues to victims, business disruption and governmental scrutiny. Sometimes, these impacts extend to businesses (banking industry) that provide payment cards to retail customers.

If the findings from the above studies are anything to go by, companies would be expected to sack hundreds of their employees every year. But sacking the employees might not be the better option to solve IIDTRC problems. Thus, the insights of these impacts of the IIDTRC incidents make it imperative for the need to proffer an effective internal data security in online retail. It reinforces the need for more comprehensive research on the prevention of IIDTRC.

1.4 Related Studies on Internal Identity Theft Related Crimes

There are few studies (e.g. Lacey and Cuganesan, 2005; Schulze and Shah, 2009) on IIDTRC prevention in the context of online retail. Existing studies (e.g. Jabbour and Menasce, 2009; Niekerk and Solms, 2010) have developed IIDTRC prevention frameworks based on the situational-oriented crime prevention approach. Some frameworks (e.g. Lupu and Sloman, 2007; Andi, 2009; Nellikar, 2010) are developed based on a sole approach of software security technology.

Others include: Systems Plan for Combating Identity Theft by Ji, Smith-Chao and Min (2008); a framework for identity fraud profiling by Jamieson *et al.*, (2008); and a model of role of Organisations in IIDTRC Response by Lacey and Cuganesan (2005). These examples and others are designed in the context of generic e-businesses. A few (e.g. Currie and Galliers, 1999) have focused on the theoretical analysis of the role of management, organisation structure and IS security. And the role of management IS security from strategic and cross-functional perspectives and the impact of management responsibilities (Earl, 1988; Betz, 2001; Rowe, 2010; Andrea and Lowe, 2009; Valrie and Rabih, 2013).

Collectively, these contributors and many others (e.g. Kaffer, 2010; Kim, Newberger and Shack, 2012), provided insights to the IIDTRC prevention practices. However, there is little or no suggested framework with grounded empirical research. For instance, Lacey and Cuganesan (2005) attempted to address the scope of e-business operations in preventing IIDTRC. They set out to resolve the challenges through a risk-based identity theft prioritisation framework. By applying theories and strategies that translate into IDTRC prevention practices, they identified the extent to which online companies can reduce data leakages. It was acknowledged that 'in interpreting and generalising their results, its limitations must be considered'. Lacey and Cuganesan (2005) noted IIDTRC prevention is a challenging issue complicated by management structure. They noted that the use of interviews and questionnaires as research approaches were not enough, since limitations of these approaches threaten their results generalisation. Lacey and Cuganesan (2005, p.260) suggest that;

> *"Further study requires a deeper understanding of organisation under study and the environment in which it operates and requires an in-depth case study for deeper understanding of e-businesses…"*

A recent study by Shah and Okeke (2012) also explores the IIDTRC prevention, by investigating the challenges faced by the IS security management of a group of UK online retail companies. Their study was based on the interviewees' perceptions. They used a Role-based model to analyse the roles of management in handling IIDTRC prevention and data security. They noted that the use of the interview as the only research approach for their research may hamper the generalisations of their findings. These suggestions emphasise that further studies need to adopt a practically oriented approach which have a rather different research designs which may help investigate how the management roles interact with the identified IIDTRC prevention practices.

These identified challenges and weaknesses – design of the studies (e.g. Lacy and Cuganesan, 2005; Shah and Okeke, 2012), the sparse of a literature on the prevention of IIDTRC in the context of online retail sector, and the IIDTRC prevention relevance suggested by researchers (e.g. Collins, 2003; Jamieson *et al.*, 2008), make the issue of how IIDTRC can be prevented in the online retail a salient research question. This research bridges these gaps in a body of literature. It builds on the suggestions by the studies (e.g. Lacey and Cuganesan, 2005; Kardell, 2007; Jamieson *et al*., 2008) that there is a need for a comprehensive IIDTRC prevention framework. And that more IIDTRC prevention research should be done from the perspective of a particular e-business with a critical examination of the management roles in handling of internal data security (Shah and Okeke, 2011).

1.4.1 Prevention of IIDTRC: The Background of Role Sharing

In 1993, the UK Department of Trade and Industry set up a Retail and Consumer Services Panel that focused on the prevention of crime arising from the online retail sector. In the report by the UK Foresight[2] (2000), this panel noted that 'well-defined partnership' and 'role sharing approach' are keys to achieving the objectives of this panel if the opportunities the 21st century world class retail sector present for UK would be achieved. It was envisaged that this role sharing approach of crime prevention should include relevant management, law enforcements agencies as well as the outsourcing companies. The concept of role sharing approach in the prevention of crimes has been established in some IS security studies (e.g. Chinchani *et al*., 2005; Park and Giordano, 2006). It has gained ground throughout the UK irrespective of the business operation, organisational structure, and institutional landscape (Crawford, 2002; Ekblom, 1994). The collaborative role sharing approach has been applied in the 1980s in other UK business organisations. For instance, the UK Home Office (1985) set up an inter-departmental working group on crime reduction. They emphasised the importance of co-ordinated approach to crime prevention in business organisations with limited crime prevention resources. This approach was conceptualised because most crimes incidents are not reported due to privacy related issues.

[2] The UK Foresight, launched in 1993 is Government White Paper on science, engineering and technology, and Realising our Potential which brings together the voices of business, government, the science base and others to look at what might happen in the future and what we need to do now to secure long-term competitive advantage and enhanced quality of life for all (http://www.bis.gov.uk/assets/foresight/docs/retail-and-consumer-services/retail-revolution-dec-2000.pdf).

Some of the crimes incidents lay beyond the reach of the criminal justice system due to organisational policies or ethics. This approach has been also acknowledged by Home Office Crime Prevention Unit (HOCPU) who defined it as another name for the 'integrated situational-oriented and offender-oriented approach'. HOCPU recommended the coordinated crime prevention approach for any business context. They noted in circular 8/84 that the collaborative role sharing approach would be imperative for an organisational change that would impact not only on the managerial roles but also on their attitudes and procedures toward crimes prevention (UK Home Office, 1985). In the results of the British Crime Survey, Hough and Mayhew (1983) gave the role sharing approach a fresh impetus by suggesting that an organisational change in crime prevention was achievable. It could be achieved by 'bending' existing crime prevention programmes and priorities and by working together. In addition, the Crime and Disorder Act 1998 for Prevention of Crime placed a duty on the business managers and law enforcement agents. This Act tasks the businesses to develop crime prevention strategies in collaboration with relevant agencies.

Some of the companies in the UK responded to this suggestion and formed a committee under the stewardship of the UK Department of Trade and Industry and the British Standards Institute. They establish a framework to adequately secure the IS within their companies.

In 2011, the UK Cyber Security Strategy emphasised more on sharing of the roles and the knowledge of IIDTRC prevention practices across businesses as the appropriate priority for vision 2015 in promoting UK in a digital world. Only a few businesses have seemed to embrace these suggestions and attempted to develop a framework for a strategic IS security to prevent IIDTRC (Shah and Clarke, 2009). Many failed due to the possible practical implications of this approach. The implications varied in terms of organisational operations, management diversities, and different structure of internal decision-making processes. It was understood that different businesses had different operations, different views of IIDTRC (the nature, causes, methods of propagation), and what could be done to prevent them (Hope and Karstedt, 2003; Kimble and Hildreth, 2004). These issues are particularly pertinent, unique and necessary to be considered in developing an applicable IIDTRC prevention framework. And these suggestions formed the starting point of argument for this study and led to the concept of a role-based framework.

1.4.2 Concept of Role-based Framework

The role-based framework (RBF) approach draws upon the idea that a systematic and integrated practices where the key components of IS management work in unison is required to prevent IIDTRC. It devolves IS security management with clear roles in a prevention of IIDTRC to collaborate with other complementary IIDTRC prevention agencies. RBF conceptualises that independent role do not provide required possible initiatives and mechanisms for an effective IIDTRC prevention. Thus, collaborative roles sharing of relevant management are needed to counter the multi-faceted nature of IIDTRC. In such, the collective contributions of the IS security management roles' perspectives are required for IIDTRC prevention. Thus, two set of perspectives – theoretical and empirical, emerges from the extension of RBF.

First, a theoretical argument is based on suggestions by researchers (Hodgson, 2006; Lawrence, Suddaby and Leca, 2009). They suggested that the analysis of an interaction between the IIDTRC prevention management and their online environment starts with understanding both entities as an organisational configuration in the same socioeconomic setting. It extends to how they cohabit side by side with an utmost aim of greater efficiency and productivity. RBF concept builds also on Hodgson (2006) suggestion that it is not possible to carry out any analysis of how management in an organisation works without having adequate conception of what it is, and how the management interrelates with its business environment. Hence, this study uses organisational role theory (ORT) to explore these relationships; since management roles in any business operations are not defined in isolation but in a 'social or organisational net of role relationships' (Elliot, 1976; Cabri *et al*., 2006).

Second, the empirical argument is based on the concept of RBF that the effectiveness of the IIDTRC prevention framework for online retail is dependent on the clarity of the shared roles of management. Therefore, effectiveness is dependent of a clarity of shared roles the management upholds (Zhu, 2006; Biegelman, 2009; Shah and Okeke, 2011). Thus, to investigate how the management uphold their roles, the empirical study is very pertinent. So the extension of an application of RBF is based on the empirical analysis via a qualitative case study. It was carried out by investigation of the roles of management in implementing IIDTRC prevention practices synthesised from of recommended identity theft prevention practices. Although, Ekblom (2010) suggests that know-how-knowledge of the process of the crime prevention plays a central role for an implementation of a framework for preventing crimes, Redo (2002) argues that successful crimes prevention depends on understanding the context under study.

Hence, this research builds on both theoretical and empirical perspectives to cover: the integration of both the external and internal of the online retail environment for implementing IIDTRC prevention strategy; strengthening of strategic roles and other forms of collaborations across online retail management, and; adoption of strategies to consult, engage and communicate with stakeholders and employees in IIDTRC prevention. The rest of this chapter provides the scope of this research on how these perspectives were explored within the defined research scope.

1.5 Research Aim and Objectives

The studies on the identity theft in the context of the e-businesses have been carried out by a few researchers (e.g. Fichtman, 2001; Davis, 2003; Newman, 2004; Newman and McNally, 2005; Jamieson *et al*., 2008; Biegelman, 2009). In particular, the researchers cover three major perspectives: prevention (Collins, 2001; Davis, 2003; Newman, 2004; Boyle *et al*., 2007; Prosch, 2009), and detection and/or investigation (Collins, 2003; Lacey and Cuganesan, 2005).

This research covers these perspectives – prevention, detection and/or investigation, to provide a comprehensive understanding of the internal identity theft related crimes (IIDTRC) prevention. The aim is to provide a framework for prevention of IIDTRC in online retail companies. This research set out the following objectives to:

i. Provide understanding of the nature of IIDTRC in online retail;

ii. Identify a framework for prevention of IIDTRC in online retail;

iii. Evaluate the resulting framework to understand how the attributes of the framework impact on online retail companies' IIDTRC prevention practices; and

iv. Examine how the IIDTRC prevention framework can be applied to the online retail Information Systems security management.

1.6 Research Questions

To achieve the above objectives listed in 1.5, the following research questions are set out:

1) What are the causes, the methods of propagation, and the preventions of IIDTRC in UK online retail companies?

Reith (1956) suggests that the study of the nature of general criminal activities (nature of the IIDTRC in this case as suggested by Newman, 1984) within the distinct socio-economic setting, the online retail in this case, may well herald in functional IIDTRC prevention framework. Given the relative scarcity of literature on the IIDTRC prevention in online retail, this research question is imperative. The motive is that an understanding of the nature of IIDTRC would help to synthesise a strategy to prevent these crimes. This question, however, is not designed to provide 'every' answer to the nature of IIDTRC in the retail industry. The central focus is to provide the explanations of the nature of IIDTRC for online retail companies that have operational IS management regardless of size, business culture and management. It is certainly the case that some distinctive features of crimes preventions in e-businesses were identified, that are relevant to the understanding of how crime prevention management works in this context.

2) What framework can be used to prevention IIDTRC in online retail?

This question flows from the question (1). Without the understanding of the nature IIDTRC in the online retail, it might not be possible to provide a comprehensive IIDTRC framework. Researchers (e.g. Gilling, 1993; Smith and Laycock, 1985; Pease 1985) have suggested that the preventive crime framework should be grounded on sound information about the crimes in relation with context under study. This question is set out to provide a framework based on theoretical analysis of an organisational role theory (ORT). It synthesises the contribution of Information Systems management roles in a prevention of IIDTRC in online retail with the concept of ORT. In doing so arrived at role-based framework (RBF) for IIDTRC prevention. As suggested by Gladstone (1980), crime prevention framework in the context of any business should entail a rational managerial role process. Gladstone added that the nature of a management of specific crime should be studied as fully as possible. In a further analysis of this question, as suggested by Emory and Cooper (1991) that breaking of research questions into simple forms may improve understanding of the question, the Question (2) was answered by addressing two additional research questions:

2a) **To what extent do the attributes of the framework influence the internal identity theft related crimes prevention practices?**

2b) **To what extent do the IS management influence the effectiveness of identity theft related crimes prevention framework implementation?**

These two investigative questions were answered to provide the background for the third research question.

3) How can online retail companies achieve a practical IIDTRC prevention with respect to the attributes of the resulting IIDTRC framework?

This question is set out to extend the use of the role-based framework by applying it in selected cases of UK online retail companies. Researchers (e.g. Jendly *et al.,* 2010; Homel, 2010) suggest that a study of crimes prevention, as it is in this case, should entail an empirical examination of the recommended strategies. Others (Homel *et al*., 2007; Anderson and Tresidder, 2008) suggest that IIDTRC prevention framework evaluation will enhance its applicability and generalisability. Thus, by providing the answers to these three research questions, this research aims to provide a strategic IIDTRC prevention framework for online retail companies.

1.7 Research Design and Methodology

A variety of research methods was considered, a qualitative case study was adopted as most suitable (Glaser, 1978; Yin, 1994; Glaser, 2001; Yin, 2003). It includes an archival research followed by a semi-structured interview and participant observations. These approaches were used for data collection to increase validity and to utilise triangulation (Vinten, 1994; Baxter and Jack, 2008). The research activity was carried out in three years – between 2011 and 2013. The research started with a review of the literature on the key concepts of identity theft related crimes in online retail. The review findings helped to refine the research aims, the research scope and the research questions. The review was followed by a case study of 4 selected online companies in the northwest of UK.

Three case studies were preceded by an initial case study. The field research also drew in managerial perspectives through British Retail Consortium (BRC)'s Retail Crime and Loss Prevention conferences. The following sources of data were drawn in this research;

(i) Archival analysis of online retail companies' IIDTRC case reports.

(i) 15 semi-structured and 7 convergent interviews;

(ii) Observation of the working of the IS auditing (ISA) of 3 online retail companies;

This research is framed by constructive and interpretive paradigms so that the selected research methods had to be compatible with and reflect these philosophical views. While the interpretive concept enabled the researcher to affirm the significance of the participants' knowledge of internal identity theft related crimes in an online retail, the constructivist concept enabled the researcher to make assumption about much complex behaviour of the subjects being studied. And that this knowledge 'subjects' possess has important consequences for how behaviour or actions are interpreted.

This study required that all participants shared not only in the construction of developing knowledge but also had an understanding of each other's objectives of participation and underlying reasons for participation so that these could be taken into account in the data analysis and interpretation. The collected data was analysed through combination of a coding system and content analysis approach aided by NVivo10. The data was categorised based on certain themes and concepts that establish the connection between the contents of empirical data and the research objectives. Using the concept of case analysis, the collated data from the research approaches formed the basis of the research discussion.

1.8 Research Benefits

The outcome of this research would be relevant to the researchers, business managers, and government and law enforcement agencies. It would help them to deploy effective Information Systems security mechanisms and IIDTRC prevention strategies to protect business Information Systems (IS) assets in online retail. To the academics and researchers, this research will help to:

i. Identify an appropriate reference theory for studying the roles of the IS security management in implementing the practices for prevention of identity theft relate crimes.
ii. Describe the impacts of management roles on effective IS practices for prevention of internal identity theft related crimes.

iii. Provide the critical analysis of the IS management roles on effective internal data security and operation.
iv. Provide a background for research in internal identity theft related crimes prevention and cyber security related studies.

To the business managers and IS security managers, this research will provide:

i. A comprehensive framework for prevention of internal identity theft related crimes, which can be used for IS security governance and operations.
ii. A strategic model of internal identity theft related crimes practices for IS security compliance management.
iii. Practical analysis of the management roles and attributes which may impact on IS security implementation in the prevention of IIDTRC in online retail companies.
iv. Options of the internal data security practices to counter internal identity theft related crimes prevention challenges face by the IS security management.

1.9 Thesis Outline

The rest of this thesis is structured as follows; Chapter 2 reviews the literature. It begins with the concepts of IIDTRC, the nature of IIDTRC – the trends of IIDTRC, the mechanisms of IIDTRC and methods of prevention of IIDTRC. Chapter 3 synthesises lessons learnt from the literature review of Chapter 2 to conceptualise role-based framework (RBF) and builds the RBF concepts on Organisational Role Theory (ORT). Chapter 4 looks into Information Systems (IS) research philosophy and paradigm which underpin this research methodology. In addition, the choice of research methods, their relevance and designs in this research are discussed. Chapter 5 discusses data collection protocols of the four online retail companies that were investigated. Each case study is taken in turn and the collated data are analysed and summarised. Chapter 6 discusses the results of the findings of the chapter 5, based on the attributes and concepts of the RBF. Chapter 7 summarises the discussions provided in Chapter 6 in relation to the propositions of RBF; and looks at their research implications and recommendations. Chapter 8 concludes the research by presenting both the theoretical and practical contributions of this research, limitations and areas of further research.

Figure 1 below depicts the design and stages for the 3 years of this research.

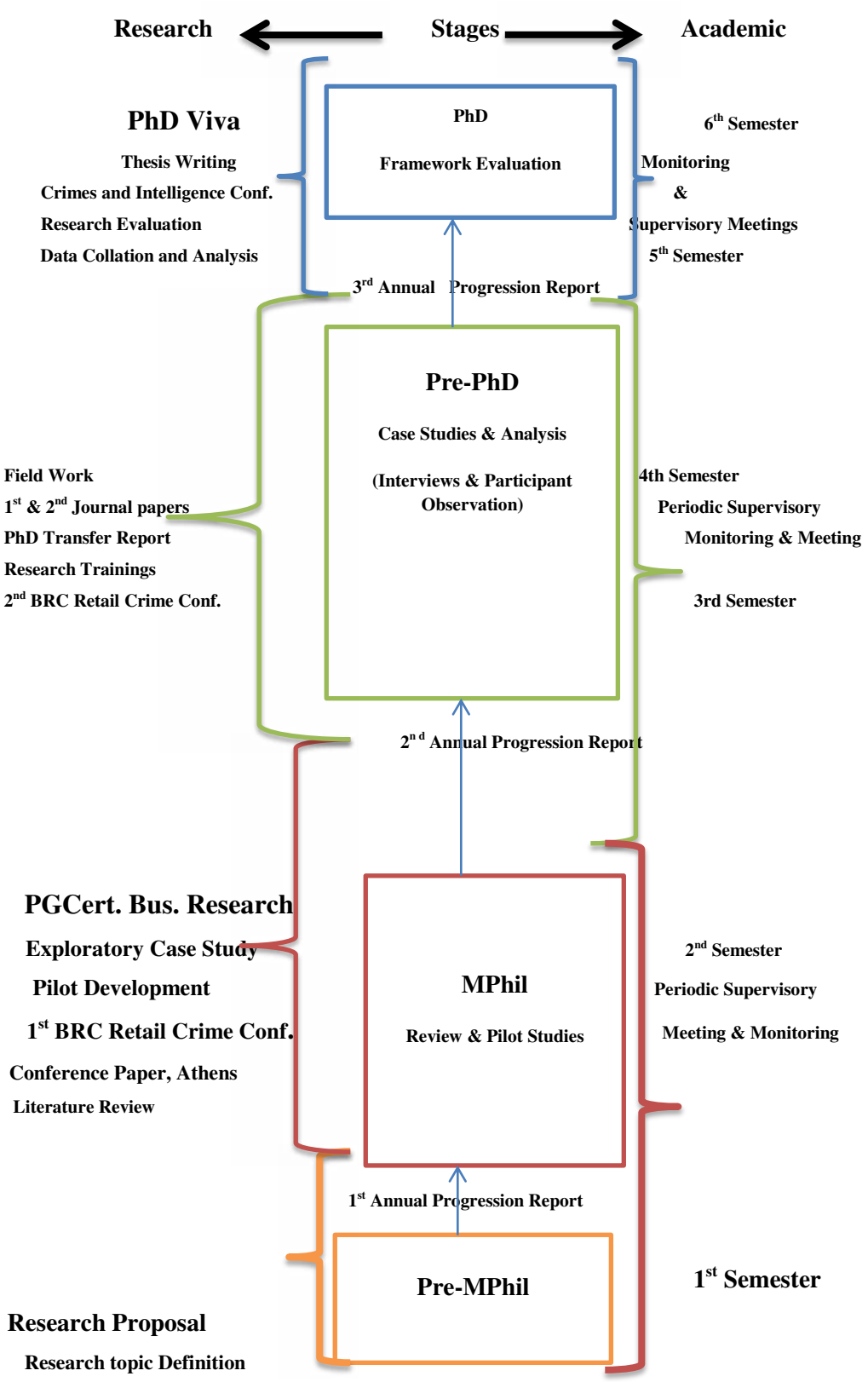


Figure 1: Research Design

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews the nature of internal identity theft related crimes (IIDTRC) – the causes, the mechanisms of propagation, and the methods of IIDTRC prevention in the context of the online retail sector. In particular, it provides the review of the scopes of the nature of the IIDTRC that motivates their prevention in online retail. This chapter locates this research aim within the related studies of IIDTRC prevention, thus ensuring it is properly targeted. Most of studies cited were conducted in the UK with a few from other countries. This chapter concludes with lessons learnt from the review.

2.1.1 Literature Review Framework

This review is designed to explore the place of this research problem in the existing literature. The review provides a step towards the study and the understanding of the role of the online retail companies in preventing IIDTRC. It was carried out through the general internet search. See the Appendix 1 for the Review Framework and Search Strategy. Some relevant case studies and reports were garnered from the UK Credit Industry Fraud Avoidance System (CIFAS), the UK National Identity Fraud Prevention and the Chartered Institute of Personnel and Development (CIPD). A few unpublished reports of internal identity theft related crimes (IIDTRC) incidents across online companies are also included without revealing their identities. Figure 2 below depicts the review framework: concepts of IIDTRC, the nature of IIDTRC and the prevention of IIDTRC. The syntheses of the review framework are centred on this research aim to provide a framework for IIDTRC prevention.

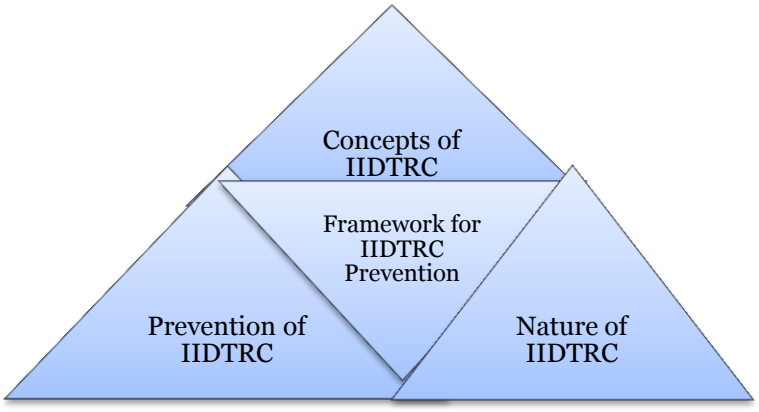


Figure 2: Literature Review Framework

The rest of chapter 2 is structured as follows; 2.1.2 extends the research background that has been introduced in Chapter 1. Section 2.2 discusses concepts of internal identity theft related crimes: definitions and themes. Section 2.3 explores the nature of internal identity theft related crimes at the workplace. Section 2.4 explores and discusses perpetration of internal identity theft related crimes. Section 2.5 provides a review of techniques for prevention of internal identity theft related crimes. Section 2.6 looks into identity theft related crimes prevention frameworks. Section 2.7 explores identity theft related crimes prevention theories and Section 2.8 summarises this chapter

2.1.2 Review Background

The prevalence of the IIDTRC in the UK online retail sector has lots of socio-economic impacts. The costs of these crimes are inestimable. It ranges from the financial cost of preventions, increasing records of brand damage, costly customers' account repair to Information Systems failure. While some studies (e.g. Gill, 2011) suggest that the current global economic crisis may have contributed to the increasing IIDTRC incidents, Schulze and Shah (2009) have noted that IIDTRC is the fastest growing crime in 21st century. These growing incidents of IIDTRC have contributed to the IIDTRC prevention's research relevance. Though, there are some studies on the prevention of IIDTRC, the application of these studies remain doubtful. This is because most of these studies are developed without empirical consideration of the business culture, settings, and operations. Some of the IIDTRC prevention frameworks are designed to protect online retail businesses from the external identity theft related crimes. They neglect 'within the companies'' activities of dishonest employees who steal and leak the identity data (Collins, 2003).

The implications of the negligence contribute to the increasing in incidents of stealing the identity properties, violation of identity protection policies, and mismanagement of biometrics data. For instance, decades ago, 62 per cent of employees committed IIDTRC in the online retail as compared to 33 per cent of hospital employees, 28 per cent of manufacturing industry (Greenberg and Barling, 1996). Recent research (Collins, 2003) holds that there is no significant reduction to these figures. Based on 1037 cases analysis of identity theft related crimes in businesses, it is noted that as much as 70 per cent of all identity theft are committed in the workplace by the employees or their collaborators (Collins, 2003).

There are few published studies on a framework for prevention of IIDTRC in the context of online retail. A few studies (e.g. Andi, 2009; Bielski, 2008; Gates and Jacobs, 2008) have focused on the theoretical analysis of impact of management responsibilities, technological incentives and public sector involvement in mitigating IIDTRC. Other studies (e.g. MacInnes, Musgrave and Laska, 2005; Anderson, Durbin and Salinger, 2008) focused more on the examination of the enormity of the problems of IIDTRC rather than on the prevention.

For instance, MacInnes, Musgrave, and Laska (2005) presented a model that identifies five causes of identity theft and related crimes: the incentives of the criminals, the characteristics of victims, the role of technology, the role of enforcement and the system related factors. They only developed a framework to determine the level of sophistication of these crimes. This model integrated these causes based on technical and non-technical factors without empirical suggestions of the model application for IIDTRC prevention. Some studies (e.g. Le Lievre and Jamieson, 2005; Jamieson, Winchester and Smith, 2007) deal with scientific approaches and techniques that only are implementable in computer systems. For instance, Le Lievre and Jamieson (2005) designed a Model of Identity Fraud Profiling. While this model is implementable on the computer systems and contributes toward understanding of the way personal documentation and information is obtained by perpetrators, it suggests little on the use of the model for IIDTRC prevention.

However, these works contributed to a body of a literature for the prevention of IIDTRC by identifying some key issues of identity theft related crimes, there are still research gaps in a body of literature in the context of distinct business sector like online retail. The issues of the dearth of a comprehensive research make the availability of the preventive mechanisms for IIDTRC remain elusive.

Researchers (e.g. Anderson, Durbin and Salinger, 2008; De, 2004) suggested that the attempts to develop solutions for the prevention of IIDTRC are hindered by issues related to: inappropriate definitions of identity theft, constraints in the form of cost and benefits in commercial business, privacy related issues, lack of understanding of the causes. Other barriers originate from legal entities and from the attitudes of managers that use incidents of IIDTRC as competitive advantage in companies affected by identity theft (Anderson, Durbin and Salinger (2008). There is also the case of the prohibition of unlimited data sharing between retail online companies by the legal bodies (Boyle *et al.,* 2007).

Anderson, Durbin and Salinger (2008, p. 172) conclude that;

> "*Both the empirical and theoretical literatures on internal identity theft related crimes are in their infancy*"

These hindrances have contributed to complexity in the prevention of IIDTRC in online retail companies; demanding new approach from both the researchers and stakeholders. Hence, there is a need for clear roles to be given to Information Systems security management team on how to enhance and implement data security strategies (Shah and Okeke, 2011). Researchers (e.g. Hosein, 2008; Salifu, 2008) suggest that identity theft has become a global issue that requires the full cooperation and participation of researchers and businesses.

This research agrees with the researchers (Shah and Okeke, 2011; Salifu, 2008; Lacey and Cuganesan, 2005) and used this review to provide the background for the extension of the role-based framework (RBF) for prevention of IIDTRC. It explores the theoretical construct - Organisational Role Theory that underpins attributes for the Role-based Framework. This review looks into the nature of IIDTRC to understand the role of management in the crimes prevention.

2.2 Concepts of Internal Identity Theft Related Crimes: Definitions and Themes

The search for an applicable framework to tackle internal identity theft related crimes (IIDTRC) may not yield a tangible success if there are no conclusive terms for defining themes related to the crimes. The need for the consensus on the definition of IIDTRC is imperative to proffering of the crimes prevention. Researchers (Lanier and Saini 2008; Koops *et al*., 2009) suggest that the problem of establishing general accepted definition of IIDTRC is that different individuals from different business operations have different concepts of the crimes. Others seem to be subjective to different ideas and experiences when they discuss IIDTRC.

In particular, Koops *et al*., (2009) noted that the generic or contextual meaning of IIDTRC is necessary, if not a sufficient factor in the study of IIDTRC prevention; and for the data security experts, the nature of propagation of these crimes is more important than the contextual meaning. Hence, there is need to underpin the concept and terms surrounding the theory of identity and its value.

Raab (2008, p.3) expresses the concept of identity as follows;

> *"Identity and identification are not just specialist terms used only by researchers in our various technical discourses…..there is enormous and diverse literature that surrounds the term identity testifies to the growing importance of identity in the politics and social life of our time…, a fixed identity may be necessary if we are to function in daily life, and history attests to the severe difficulties that befall persons whose 'papers' have been destroyed or confiscated, and who therefore need to construct an identity…"*

The concept of identity, as it is in the context of most social theory, influenced the context of its discussion and analysis. Josselson and McAdams and Lieblich (2006) examined identity and state that: *"identities are not fixed and frozen" as individuals evolve in time"*.

As defined by Burke (2008, p.2), An Identity

> *"is a set of meanings applied to the self in a social role or as a member of a social group that define who one is"*

Koops *et al*., (2009) express identification of individual as it attributes to self is a vital element of identity explanation. They distinguished identity between 'Idem Identity' and 'Ipse Identity', as the 'sameness of persons or things', and 'personal identity in the meaning of an individual sense of self' respectively. This concept 'idem identity' is adopted in rest of this study. IIDTRC are committed against what make an 'individual unique', and this 'individual unique' is what Goffman (1990) termed 'Identity pegs'.

2.2.1 Definition of Internal Identity Theft Related Crimes: The Contextual Issues

As the definition around the term 'identity' is not straight-forward so is definition of the IIDTRC. The tactics adopted in this research is to deduce relevant questions to simplify the understanding of the complexity of defining internal identity theft related crimes. The basic questions that constitutes important elements in defining IIDTRC are: who are individuals or groups that commit the IIDTRC? Where are IIDTRC committed? When are IIDTRC committed? On the issues of the place and circumstances surrounding the crimes, the definition of identity theft related crimes could be extended to the online retail as an organisational entity with respect to management and operations within the organisations.

The distinctiveness of internal identity theft related crimes is also imperative to consider in considering the issues of the identity theft definitions. This is because an extensive number of different crimes often include the use or abuse of identity. Such crimes include financial fraud such as plastic card fraud, credit cards, cheque cards, debit cards and phone cards, etc.; as well as immigration fraud such as counterfeiting, forgery, terrorism (using false identity); and other theft of various kinds such as postal fraud, pick-pocketing, robbery and burglary, etc. As IIDTRC have different meanings to private corporations as to the public sectors, some of them argued that credit card fraud and account hijacking should not be part of identity theft as would be discussed in the various contextual definitions below. Specifically, most financial institutions do not classify the fraudulent use of stolen credit card numbers as an identity theft but as a payment card fraud (Cheney, 2005; Meulen, 2011).

To answer the above questions and provide definitions of IIDTRC, the UK Home Office Identity Fraud Steering Committee (2006) posits that Identity theft occurs when a False Identity details are used to support an unlawful activity. This position shows that the UK hardly distinguishes the definition of identity theft and identity fraud. In contrast, United States distinguishes between identity theft and identity fraud. As the cultural context in the definition of the identity is always considered alongside the region where the crime is committed, researchers from the US define identity fraud and identity theft as two distinct or mutually exclusive concepts. The US definition of identity theft crimes argues that identity fraud occurs when a perpetrator takes over a fictitious identity whereas identity theft is committed when the perpetrator takes over the existing identity (Gill and Binder, 2005).

This issue of different contextual definition of identity theft goes for a number of other countries. In Canada for instance, "theft" must involve 'a deprivation of an actual thing to the owner', thus 'copying personal information from a computer or official document for future criminal use may not be an offence under Canadian Criminal code' (Canada Countermeasure Committee, 2005).

2.2.2 Definition of IIDTRC: The Circumstantial Issues

In as much as the use of cultural perspectives and circumstances surrounding IIDTRC can be helpful to researchers in understanding the nature of the crimes, the term 'identity theft-related crimes' is generally in most literature (Meulen, 2011).

Many States, Commonwealth Agencies and Territory consistently interchange the use of the terms 'identity fraud' and 'identity crime'. Definition of 'identity theft and identity fraud' as put by the Federal Identity Theft and Assumption Deterrence Act USA, UK Home Office, and some researchers might not be an acceptable or a viable option. This is the reason for general belief that the definition of identity theft related crimes should be considered irrespective of its terms, location, region, and cultural background. Though, they argue that the most relevant issue is to explore the elements of these crimes and relate them to the circumstances surrounding its occurrences with particular business as an organisational entity.

According to the United Nations Intergovernmental Expert Group (UNIEG) cited in Organisation for Economic Co-operation and Development (OECD, 2008), the term 'identity fraud' 'the element of deception' lies not only in the deception of technical systems and human beings to obtain the fraud but in deception of victims in the subsequent use of the stolen information. However, there is still no standardised definition in the field of offences related to the theft of identity. As noted above, American literature always adopts the term identity theft, while UK (HM Cabinet Office, 2002) and other countries these offences are termed identity fraud. This difference in defining identity related offences is still a big challenge in resolving the problem as noted by Koops *et al.,* (2009, p.4) in the statement:

> *"...It is also not clear what exactly constitutes 'identity theft' or 'identity fraud' and how these can be combated ... This lack of precision becomes especially apparent when comparing the various official media reports on these topics. Definitions are hardly ever provided, even though the statistics play a role in politically motivated discussions and policy decisions. Commonly accepted definitions are also lacking in the literature. This means that we are at the stage where comparisons of apples and oranges abound making it virtually impossible to determine the real incidence of identity-related crimes..."*

Currently, the commonly cited definitions (though some could not be cited without critics) of identity theft are as follows: "*An individual is considered to commit an act of identity theft when he or she "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law"* (Federal Identity Theft and Assumption Deterrence Act USA, 1998*, title 18 United States Code - Section 1028).*

The UK Home Office defines identity theft as an act which *"occurs when sufficient information about an identity is obtained to facilitate Identity Fraud irrespective of whether, in the case of an individual, the victim is alive or dead*" (Home Office Identity Fraud Steering Committee, 2006). In more extensive approach, the UK Fraud Advisory Panel (2011, p.1) states that the

> '*Identity fraud' is commonly used to describe the impersonation of another person for financial gain. Fraudsters steal your personal identity and/or financial information and use it to purchase goods and services or access facilities in your name…, it is the use of a false identity or another person's identity to obtain goods, money or services by deception. This often involves the use of stolen, counterfeit or forged documents such as passports, driving licences and credit cards.*

In the Australasian Centre for Policing Research, James (2006, *p.iii*) defined identity theft as;

> *"the theft or assumption of a pre-existing identity (or significant part thereof) with or without consent. It may involve an individual's identity (whether a person is dead or alive), or the identity of a business"*

The OECD (2008) expresses the similarity in the definitions in the analysis that: 'Identity theft' is a subset of identity fraud and that both 'Identity fraud' and 'Identity theft' are a subset of identity crimes. This analysis is depicted (see figure 3) by the Koops and Ronald (2006) framework in which they include identity fraud and identity crime in one umbrella term 'identity related crime'. From the above elaborated discussed definitions, it is worth noting that identity theft related crime encompasses the unlawful use of the identity of both the non-existing and existing persons. Due to the logical analysis of these terms: 'identity theft, 'identity fraud' and identity theft related crimes', this proposed definition by both OECD (2008) and Koop *et al.,* (2009) provides perhaps most widely cited reflection of the relationship between identity theft, identity fraud and related crimes. This definition is arguably considered by researchers as the most useful, since it encompasses additional elements of IIDTRC.

Figure 3: Identity Theft Related Crimes Definition Framework
(Adapted from Koops and Ronald, 2006)

The precise framework for defining identity theft related crimes which include both identity fraud and identity theft is based on the following suggestions by OECD (2008) and Koop *et al.,* (2009) that:

i. Identity theft related crimes concern all punishable activities that have identity as a target or a principal tool.
ii. Identity fraud is unlawful activity where an identity of an existing person is used as a target or principal tool without that person's consent.

Moreover, the contextual range of identity theft related crimes are much broader, and they are certainly significant as the definition is unrestricted to any particular context. This definition buttresses the point made by Gerring (2001, p. 54) that,

> "*A concept that applies broadly is more useful than a concept with only a narrow range of application'. A good concept stretches comfortably over many contexts; a poor concept, by contrast, is parochial – limited to a small linguistic turf*"

In the same vein, the IIDTRC definition framework developed by Newman and McNally (2005) describes identity theft related crimes' in three phases. The different phases are: T_1, T_2 and T_3 which means the time (T_1) of acquiring the personal identity information of the victim, the identity theft action (T_2) and the outcome of the identity theft (T_3) respectively. The above framework by Newman and McNally (2005) could help guide researchers on searching for the preventive strategies on identity theft and to establish a better definition.

2.2.3 Summary of Concepts of Internal Identity Theft Related Crimes: Definitions and Themes

Though, there are other terms used by the researchers to describe identity theft related crimes such as 'identity deception' – which arguably is not widely recognised since the term 'deception' is negligence of the role of the victim whose identity is stolen (Wang, Chen and Atabakhsh, 2004). Nevertheless, the definition of IIDTRC in the context of this research is the 'unlawful manipulation' of technical systems as well as human beings by the dishonest or disgruntled employees to steal another person's identity to commit criminal offences. This research would use this definition as the basic references for the subsequent sections.

In addition, the Australasia definition of identity theft cited by James (2006) is incorporated throughout identity theft related crimes references made in this study because it covers not only the concept of human identity but also the identity of business. The next section explores some of the research theories, which provide answers to the questions of the nature of IIDTRC as it is underpinned by the characteristics IIDTRC perpetrators. It discusses some vital theories that provide some interesting answers on 'why' motivations of the IIDTRC perpetrators based on 'how', 'when' and 'where' these crimes are committed. The answers provided in the next section are in-line with the provisions of the first objective of this research: understanding of the nature of IIDTRC in online retail.

2.3 Understanding Internal Identity Theft Related Crimes at the Workplace

Several researchers (e.g. Cressey, 1973; Ditton, 1977; Mars, 1982; Mars 2006; Gill, 2011) have used theories to provide comprehensive conceptual understanding of workplace crimes: how crimes are perpetrated at work place, how organisations adapt to the crimes and why the perpetrators act in certain ways. The theories discussed in this section provide this research with different 'lenses' through which to look at the complex problems of internal identity theft related crimes (IIDTRC). For instance, some theories (e.g. Mars, 2006) focus attention on different aspects of the issues of occupational deviance: cheating, fiddles, pilferage, scams and sabotage in the 21st century and providing a framework within which to conduct their analysis in relation to IIDTRC. The analysis provides understanding of the nature of IIDTRC from the context of occupational crimes and related it to online retail companies. This section contributes to the understanding of nature of IIDTRC by providing answers to the question of 'why internal identity theft related crimes' in the online retail. Thus, contributes to meet the first objective of this research.

2.3.1 Internal Identity Theft Related Crimes: Workplace Dishonesty

The evolution of the digital economy and changes in the technology has direct impacts on the nature on workplace crimes. The computer-related crimes; the internal identity theft related crimes in this context are not the exception. Mars (2006) notes that the even though the extension of information technology has undoubtedly reduced employees' controls in some jobs, it has radically increased their controls in others.

In his anthropological study of occupational crime, Mars (1974) applies Douglas's (1970) concepts of 'grid' and 'group' to classify the occupational structures in relation to workplace deviance. He divides employees in four categories based on the structure of their occupations. The first category is 'the Hawks', the workers who manipulate organisational rules for their own advantage. The typical examples of such workers are 'the entrepreneurs, the innovative professionals and the small business owners'. Second category is 'the Donkeys'. The Donkeys are highly constrained by rules. They respond to the systems that constrain them by breaking them, 'to fiddle or to sabotage the systems'. The third category is 'the wolves'. Mars (1974, p.2) expressed this category as '*the dockwork gangs'*, or 'the work-and-pilfer'. They work in well organised and highly regulated packs.

Fourth are 'the vultures'. Examples are writers and traveling salesmen who commonly work supportive and corporative base. They are highly competitive and individualistic, fiddle in ways which, because of the nature of their jobs. These above categories which emerge from the Mars' (1974) study shows 'cheats', 'fiddles' or 'sabotages' as being multifunctional. Mars (1974) suggests that workers under different respective categories engage in dishonesty or criminal acts to make 'unequal reward systems as a bit more even'. He cited instances, 'the fiddles' justify their act: as being indicators of occupational success and status, as satisfying punitive measures against employers, as being antidotes for boredom, as ways of avoiding the delays and perceived injustices of clumsy bureaucratic systems, and ways of increased control at the workplace.

Mars (1974) overall suggestion is that 'the dishonesty' at the workplace should be seen as being more than an index of employee dissatisfaction, that it should be seen as pointing to ways in which the criminal activities could be changed to bring employees into the centre of workplace control. Specifically, Mars (2001a) suggests that increases in the control over the 'the Grid Donkey jobs' – as in the call centres of the today's online retail companies, for example, encourages dishonesty and deviance, particularly resentment fiddles. Information technology, paradoxically, increases the power of dishonest employees who if disruptive can be resentful and prone to indulging in sabotage. In his agreement to the above contentions by Mars (2001a), Hollinger (1997) points out that behaviours of the dishonest employees in this computer age represent merely a 're-tooling' of deviant and criminal activity. In order words, sabotage as a form computer related crime is not necessarily a new form of sabotage but a 're-tooling of the status quo', which can be IIDTRC, as it is in this context.

Mars (2006) suggests that a response to curb the behaviours of dishonest employees categorised above do not always prove to be effective. He noted that such behaviours need collective preventive action from workplace management in form of both '*coercive technology' and 'technical up-gridding'* (Mars, p. 289).

The above analysis of Mars (1974, 2001a) shows the importance of employing broad interpretation in explaining the understanding of all workplace behaviours such as IIDTRC, and not to ignore the covert occupational institutions and systems. Mars (1974, p.204) argues that

> "*any management who introduces or proposes a change to the workplace without considering covert reward systems are operating blindfold; examine and discuss 'the way fiddles produce their own set of social relationship in the workplace and gauge the effect that any planned change would have on them."*

This suggestion, in particular, is important in this research. It underpins the rationale for exploring the theoretical analysis of the motivating factors that induce dishonest employees into internal identity theft related crimes.

2.3.2 Internal Identity Theft Related Crimes: Perpetrators Motive

Researchers (Clarke, 1999; Newman and Clarke, 2003; Gill, 2011) noted that there are three major factors that induce the dishonest employees to steal the personal identifiable information in online retail companies. These include: a) Perpetrators concealment; b) Financial gain and rewards; c) Business environment; d) Economic Climate – Recession

Concealment of the Perpetrators: Some perpetrators of IIDTRC in the online retail companies have mind-sets that such environment avails them the opportunity to remain anonymous. Newman and Clarke (2003) noted that this environmental factor offers substantial opportunity for crime. How this factor attribute to the IIDTRC is summarised with the acronym **SAREM**: Stealth, Challenge, Anonymity, Reconnaissance, Escape and Multiplicity, shown in the table 1 below.

SAREM	Concealment Attributes
Stealth	The IIDTRC perpetrators are almost invisible on the internet, thus a perfect condition for committing identity theft related crimes (Denning and William, 2000).

	Concealment Attributes
Anonymity	With the information system attributed with decentralised database system, anonymity abounds that allows the employees to act irresponsibly or criminally (Wortley, 1997).
Reconnaissance	This attribute is noted as perhaps the most important element that motivates criminals in most business organisations, as the information system makes it possible to scan thousands of database servers and even millions of personal computers that are connected, looking for the target victims.
Escape	This sums up other attributes owing to the crime-inducing aspects of the information system environment of anonymity, deception and stealth, thus making internal identity theft in the business organisation difficult to be detected. IIDTRC perpetrators perceive that it is easy to escape punishment (Ahuja, 1997).
Multiplicity	Unlike other traditional theft that is relatively finite in nature; internal identity theft related crimes could be multiplied exponentially since the perpetrator has access to a vast number of new opportunities to IIDTRC.

Table 1: Concealment as a Motivation for Internal Identity Theft Related Crimes

The Financial Gain and Rewards: It is a general idea that identity is a psychological construct used to identify particular individuals 'uniquely' (Cast, 2003). Identity is a construct which has invaluable attributes of every individual. This definition points that victims of identity theft related crimes (IIDTRC) have lost something more than simply just money. If an identity of an individual could be conceived as a composition primarily of information that is unique, priceless and invaluable, then one perhaps begins to understand the motivation of IIDTRC perpetrators.

Clarke (1999) has conceptualised that identity is a 'hot product' and that hot products attract theft. He demonstrated how personal identifiable information – 'hot product', can be more prone to theft than others using the acronym CRAVED: Concealable, Removable Available, Valuable, Enjoyable and Disposable, as described in the table 2.

CRAVED	Financial Gain and Reward Attributes
Concealable	From the institutionalised information systems (document lockers, intranet, and internet), one can steal personal identifiable information secretly without possessing it completely, and can do so from any accessible and convenient place.
Removable	With the intangible nature of the information of individual identities, it is thus removable, movable and intrinsically vulnerable to interception and can be disguised to any desirable and intended forms by the criminals.
Available	The revolution of the Internet has made all information potentially available to everyone. Personal information and records are there for the taking. In fact, one does not even have to steal them. One can buy identification information as cheaply, breed other identification documents from them and then convert them into cash.
Valuable	Personal Identifiable information details (e.g. credit cards, bank passwords) in this current information society (e.g. retail and banking industries) is conceptualised as money. These are such valuable items; thus the target of the criminals.
Enjoyable	For the internal identity thieves in a business organisation, there case of lure of pleasurable living and rewards whenever stolen identities of the innocent clients or customers are converted into cash.
Disposable	Sutton and Cherney and White (2013) notes that the availability of a fencing operation enhances the chances of particular items being stolen. Unlike the traditional stolen goods with the attribute of continued possession increases the risks of being caught, stolen identity and the disposal of the identity is not so apparently pressing. The criminal continues to savour the gains of the stolen identity in hidden until the crime is detected.

Table 2: Financial Gains as a Motivation for Internal Identity Theft Related Crimes

The Business Environment: Motivations in a workplace may be perceived as predispositions to particular behaviours and outcomes, reflecting the things employees want and the strategies they may choose to achieve it (Thompson and Mchugh, 2009).

Researchers (e.g. Newman, 2004; Lacoste and Tremblay, 2003; Slosarik, 2002) have identified business environment, such as online business (online retailing) as the major source that provides opportunity for individuals indulging IIDTRC. They classified the sources into two: (1) The collection centres and (2) The application centres. The Collection Centres/Point in a business environment is where the criminals steal personal identifiable information while the Application Centres is the point of use. Examples of the collection centres include business office via company databases and paper or electronic documents, business transaction via workplace environment and personal computers, financial statements via credit/debit statement and internet, and data mining via abetted hacking. Moreover, other researchers (Davis, 2003; Morris II, 2004; Newman, 2004) summarised categories of IIDTRC perpetrators in relation to the online business environment. They classify the criminal attributes of IIDTRC perpetrators based on their criminal activities as described in table 3.

Category	*Characteristics*
Incidental	These are the amateur IIDTRC perpetrators that take advantage of varied incidences – data leakages within the IS, without any specific task-based intention (Perl, 2003).
Opportunistic	Amateur criminals with intention, without taking any risk. These criminals are not professionals; though, they look for opportunity; if they get any, they would take it. In some cases they are referred as the circumstantial or secondary identity thieves. These criminal often advance to professional because of interest and financial gain from the initial act (Davis, 2003).
Professional	These are criminals with learned techniques with an in-depth knowledge of various methods to perpetrate IIDTRC (Morris II, 2004).
Gang	These are criminals in form of organised group, comprised of several experts from suitable fields (e.g. Computing, Psychology). This form of thieves is offensive with high level of commitment (Newman, 2004).
Seller	These are IIDTRC perpetrators that sell identity information such as credit/debit cards, e-mail address, driver's licence, home address, etc.

Table 3: Features of Internal Identity Theft Criminals

Economic Climate – Recession

Gill (2011) argues that there is some evidence that characteristics of an adverse economic climate can lead to either an increase or a decrease in crime. Gill suggests that since there is a possibility of the unavailability of credit due the recession, there is likelihood that such economic climate will create opportunities for fraud. Leslie and Hood (2009) agree with Gill (2011) and argue if dishonest employees have less disposable income during recessions due to redundancy during recessions they would motivated to indulge into IIDTRC. In contrast, Yeager (2007) argues that there should be caution in supporting the hypothesis that recession leads increase in crimes. Gill (2011) also cautions that care should be taken in generalising his suggestion since different crimes are influenced by different issues.

Gill (2011) and Yeager (2007) agree that further research need to be done to assess the frauds patterns that may have a significant impact during the recession. They suggest there is need to look into other theories that discuss the criminal motive that influence the increase in crimes. Other researchers (e.g. Kantor, 1983; Black, 1987; Brooks and Kamp, 1991; Kardell, 2007; Clarke, 2009) have used theories to analyse other motivating factors and situation that could induce employees to perpetrate IIDTRC. The relevant concepts considered are;

- Cressey's Fraud Triangle;
- Person Theory;
- Workplace Theory.

It is important to look into some of the theories that motivate crimes because they provide an analytical explanation of employee's behaviour based on the key elements: environments, situations and time. These elements (environments, situations, and time) answer the key questions of where, when, why, and how as they relate to the nature of internal identity theft related crimes.

Cressey's Fraud Triangle Model

Cressey (1973) in his theory of 'the triggers' that lead to crimes pointed out that each criminal have motives and opportunities that induce them to commit crimes. He models a 'Fraud Triangle' of which each side representing components of what causes the perpetrators to commit crimes. The three components are Rationalisation, Perceived Opportunities and Social Pressure facing the individuals.

Cressey (1973) explained that the rationalisation and social pressures are the key attributes motivates the employees attitudes towards crimes. Kardell (2007) also suggested that while perceived opportunities might be managed by the organisations, rationalisation and social pressures are generally beyond the control of the organisations.

Person Theory

This theory uses the concepts of Opportunity, The Marginality Proposition, and Epidemic of Moral Laxity to explain why some employees may indulge in IIDTRC. This theory could be extended to the prevention of IIDTRC. The summary of the interpretation of these approaches is presented in table 4 below.

Person Theory's Components	**Explanation of the Pearson Theory in relation to concepts of Internal Identity Theft Related Crimes**
Opportunity	Cressey (1973) and Kantor (1983) claim that opportunity correlates positively with IIDTRC. In agreement Kardell (2007) argues that minimised opportunity like constant surveillance over employees' activities could be IIDTRC-deterrence. This theory pointed out that employees are naturally greedy. And this could be translated to crimes if there is an opportunity at the employees' disposal.
Marginality Proposition	This approach holds that the employee's degree of marginality could the cause identity theft related crimes within organisations (Clarke, 2009).Social isolation, little opportunity for advancement, short tenure, low rank in the organisational hierarchy, low wages, expendability, little chance to develop relationships, etc. are characteristics of the marginal employees. Employees that fall in this category are more likely to indulge in IIDTRC (Barling, 1995).
Epidemic of Moral Laxity	This approach postulates that moral decadence in the society today leads to moral laxity in the organisations (Clarke, 1999). Newman and Clarke (2003) support this concept and suggest that employees of decades ago possess better trustworthy qualities than the employees of today.

Table 4: Analysis of IIDTRC Motivating Factors with Persons Theory

Workplace Theory

This theory contributes to explaining the reasons some businesses, the online retail companies in this case, suffer higher levels of internal identity theft related crimes. Hence, the analysis provided by the workplace theory, which is situation specific, could lead to the evaluation of different systematic strategies for controlling and preventing IIDTRC. Workplace theory explains the motivation of disgruntled employees that engage in IIDTRC based on the concept of Workplace theory shown in table 5 below.

Workplace Theory	***Explanation of the Concepts of Workplace Theory in the context of Internal Identity Theft Related Crimes***
Perceived Fairness	This model points to a relationship between employees and perceptions of organisational fairness. Tucker (1989) notes that IIDTRC can be better characterised as a mode of social counter-control rather than a crime. In this model context, the incidences of IIDTRC are seen as a response to the perceived deviant attitude of the employee (Black, 1987). This theory argues that exploitative behaviour of an employer as the cause of the stealing. Hence, employees' admissions of IIDTRC might be associated with job dissatisfaction.
Climate and Structure	This approach is suggested by Brooks and Kamp (1991). It argues that dishonest organisational climate encourages dishonest attitude (Johns, 1987). Employees' perceptions about the work climate, their co-workers, attitudes of their supervisors and management; can send messages to them whether the crimes could be condoned or not. Shearman and Burrell (1988) note that structure of IT and information system security and IT affects the propensity of employees stealing the organisation data. The more complex is the security of the information storage, the less propensity of loss and incidences of IIDTRC.
Deterrence Doctrine	This approach holds that IIDTRC will be more likely to be perpetrated in an organisation where there is low awareness of anti-crime policies. Kantor (1983) supports this approach that employees' behaviours are influenced by threat of organisational sanctions. According to Greenberg and Barling (1996), the most effective variable of this approach in deterring IIDTRC is the perceived certainty of punishment among other variables: perceive severity and visibility of punishment.

Table 5: Analysis of Motivations of IIDTRC with Work Place Theory

2.3.3 Summary of the Understanding of IIDTRC

This section has provided the review of the related works on the theories and concepts of the nature of internal identity theft related crimes. It has identified the importance of these theories in understanding the motives of perpetrators of IIDTRC. The above review provides answers to the question of 'why internal identity theft related crimes in the online retail companies?' in relation to the research question of the nature of IIDTRC. Thus, contributes partly towards understanding the first objectives of this study: to provide understanding of the nature of IIDTRC in online retail. The next section will review studies on the perpetration of the IIDTRC. It provides understanding of: who; how and when IIDTRC are perpetrated, and who detect the crimes in relation to their prevention.

2.4 Perpetration of Internal Identity Theft Related Crimes

With the growing the internal identity theft related crimes (IIDTRC) in online retail, researchers and stakeholders continues to as ask: why are the IIDTRC a growing risk? To answer this question, it is important to reflect on the motivations for the activities of the IIDTRC perpetrators discussed in the section 2.3. Rationalisation, opportunity and social issues are the key motivating factors for perpetrating IIDTRC. A greedy (social issue) employee working in an unsecure IT infrastructure (opportunity) believes (rationalise) that s/he may not be caught for indulging in IIDTRC. The perpetrators would be motivated to act because of the nature of the online retail business operation which is carried out using the internet – activity behind the computers.

Other motives include gambling lifestyle or pressing bankruptcy and debts. Having the opportunity to commit a crime prepares the fraudulent employee to look for the situations that would pay off. For instance some of the perpetrators, irrespective of gender, either obtain temporary employment for the sole purpose of personal or business identity thefts or place organised criminals in the business organisations to gain knowledge of the firms' information systems in order to commit their frauds.

Hinds (2007) suggested that the structure of the firms' Information Systems and Data Protection Policy are among the key enabling elements that may encourage IIDTRC. The elements are interrelated that one situation or an opportunity for the IIDTRC perpetration leads to the other.

2.4.1 Enabling Elements for Perpetrating of IIDTRC

Researchers (e. g. Collins, 2006; Duffin *et al.,* 2006) suggested that the perpetrators of internal identity theft related crimes (IIDTRC) often target and exploit weaknesses in online businesses operation because of the structure of the information systems and the business policy.

The structure of Information System: The modern information systems architecture of online retail is designed to store the customers' data in one place which could be accessible to employees in a variety of departments. It is generally built with a structure of distributed information systems in which networked computers communicate and interact with each other to achieve the common goal of their business transactions. This design may result to a consolidation of diverse customers' information that might be of easy access to the fraudsters (Duffin *et al.,* 2006). It makes it easier and quicker for perpetrators to have the comprehensive information of the customers' data at a glance. This structure also creates opportunities for the organised criminals to target employees in the information system department of the retail companies.

Data Protection Policies*:* Collins (2003) cited the case of the U.S department of Justice which suggests that identity theft related crimes are escalating because of lack of definitive policy. Due to the definition problem discussed in 2.2 above, some law enforcement agencies could not record the identity theft related crimes as a separate crime. And because of the nature of the identity crimes as a cross-jurisdictional which may span or cover several geographical areas and business networks (Meulen, 2006). These suggestions might have led to confusion about who is responsible to investigate and prosecute the IIDTRC cases. In some cases, this leads to the victims of IIDTRC reporting the cases to wrong enforcement agencies. For instance in the cases of IIDTRC involving bank details, victims are likely to report the case to the financial crimes investigation agency rather than the police. Meulen (2006) in agreement with Collins (2003) suggests that the issue of undefined data protection policies and jurisdictional or management roles make the loss related IIDTRC more impactful. For instance, most outsourcing firms run into difficulty in offering an identity monitoring service for their customers because some employees within the retail companies thwart credit-monitoring processes based on the stipulations that the outsourcing firms (third party firms) are not part of their statutory data protection policy. Such circumstances contribute to the identity monitoring service arrives days after these crimes activity have transpired (Collins, 2006).

2.4.2 Mechanisms for Perpetration of Internal Identity Theft Related Crimes

Researchers (e.g. Mitnick and Simon; 2006; Endicott-Popovski and Lockwood, 2006; Hinds, 2007; Green-King, 2011) suggest that infiltration, collusion, and coercion, and social engineering are the common mechanisms IIDTRC perpetrators use to carry out internal identity theft related crimes (IIDTRC) in online retail companies. These mechanisms can be carried out independently or combined with other mechanisms. For instance, with collaboration and social engineering, combined, cyber criminals can generate the phishing web pages for nearly any online retail company at a click of a mouse or tap of a key (Dhamija, Tygar and Hearst, 2006). Financial Insights[3] (2004) cited other IIDTRC perpetration mechanisms such as botnets, PID[4] account fraud, and privacy counterfeiting. APWG[5] (2014) suggests that botnets which involve networks of IS and machines with malicious programmes in the form of phishing attacks is one of the newest IIDTRC tactics that pose internal data security threats to online retail.

APWG (2014) suggests that some of the IIDTRC perpetrators succeeded in manipulating the IS by using various techniques which include unapproved hardware/devices, abuse of private knowledge, violation of e-mail/IM/web/internet policy of the victims, handling of data on unapproved devices/media, storage/transfer of unapproved content and use of unapproved services/software (APWG, 2014). The table 6 below summarises common mechanisms for perpetrating IIDTRC.

Mechanisms	***Explanation of the IIDTRC Mechanisms***
Infiltration	This is a mechanism whereby organised criminals plant the agents in the retail companies. The planted criminals (outsourcing agents, vendors, and partners) could gain employment to commit IIDTRC. The factor behind this mechanism could be linked to the commercial pressure or high employees' turnover in the online retail (Green-King, 2011). The pressure can open door for influx of the deliberate criminals in retail outlets and call centres. Green-King (2011) suggests that less stringent vetting and recruitment controls measures encourage infiltration. This situation is often difficult to detect. The perpetrators often resign before the detection. Some criminals lease or sell the compromised data.

[3] Financial Insights, an International Data Corporation company is an independent market research and analysis firm specializing in IT media (www.financial-insights.com).
[4] Personal Identifiable Data
[5] Anti-Phishing Working Group founded in 2003 is an international consortium of organisations (includes BitDefender, Symantec, McAfee, VeriSign, VISA, IronKey, Mastercard, Internet Identity, ING Group, etc.) affected by phishing attacks (http://www.antiphishing.org)

Mechanisms	*Explanation of the IIDTRC Mechanisms*
Collusion	The organised criminals and dishonest collude with fellow employees (in some cases with dismissed employees or business partners) who have access to personal and business information systems – payroll, account details, business transactions and records, etc. It is common approach used by some criminals of the same cultural background (Hinds, 2007). The meeting point is often at lunchtimes, nightclubs, pubs and in social events.
Coercion	Organised criminals intimidate and threaten employees to partake in IIDTRC. In some cases call centres' employees of the same company are being threatened by the top managers. Some employees who involved in this fraudulent activity often claimed that they did so under duress. Successful coercion often leads to activity of collusion with the collaborators. Hinds (2007) suggests that 45 per cent of the IIDTRC cases in UK are coerced of which 15 per cent of this percentage admitted to having been paid to compromise their customers details. Some of the innocent employees (e.g. cashiers and wait-staff) were often coerced to skim payment cards. There were reported cases of recruiting the IS/T administrator for the purpose to steal data, open IS/T holes and disable security systems. Verizon DBIR (2013) indicated that pretexting was one of the common elements of social engineering modes used in IIDTRC perpetration.
Social Engineering	Act of pulling a con job to get access information system that is normally accessible by the privileged users - employees. It is the human side of breaking into an online retail Information Systems. Several researchers (Duffin, *et al.,* 2006; Savage, 2003) have noted that the perpetrators of this form of IIDTRC are often link with internal employee as an agent. This mode often involves social tactics – deception and manipulation, in exploitation of the roles of the human elements and end-users. These modes of IIDTC perpetration often linked both the technical and non-technical modes, alongside collusion of the perpetrators with external agent for successful exfiltration of victims' PID/I assets. There were reported incidents carried out by payments and promises to employees to get them indulge in IIDTRC, because these external agents deemed the IIDTRC impossible without their aid (Checkpoint, 2013).

Mechanisms	*Explanation of the IIDTRC Mechanisms*
Social Engineering	Check Point (2013) indicates that 42 per cent of the UK companies have been hit by social engineering attacks of which new employees (52 per cent), and the outsourcing agencies and contractors (44 per cent) are most vulnerable agents.
Patchable Software Vulnerability (PSV)	Verizon Data Breaches Investigation Report (DBIR) (2013) notes that PSV as one of the key mechanisms of IIDTRC perpetration. Verizon DBIR (2013) discusses the summary of the Verizon DBIR from 2008 to 2013, which shows that web applications, remote access and desktop services are the commonest pathways or vectors through which above IIDTRC were perpetrated. This report emphasises the risks of the role of human errors when the privilege users manage these vectors in online retail companies. This evidence shows that remote access and desktop services combined with exploitation of default/stolen credentials in very rampant in retail companies. It can be concluded that opportunistic IIDTRC incidents (intrusions) are common with retail companies who often share same IS/T support with software vendors. With the IIDTRC perpetrators (system administrators) knowledge of vendor's authentication methods and schema (e.g. TCP port 3389 for RDP; or TCP port 5631 and UDP port 5632), they can exploit (without traces) across full range of the vendors/partners/outsourcing companies (Peretti, 2009).

Table 6: Common Mechanisms of Perpetrating IIDTRC in Online Retail

Other mechanisms for perpetrating IIDTRC are phishing, repairmen and elaborate yarns to hoodwink the human resources staff into providing companies identity assets. The key technical modes used by the outsiders/external agents who were abetted by malicious insiders include: malware, hacking, social engineering, and physical actions. Though some online retail companies may implement elaborate authentication process, firewalls, networking security monitoring technology and virus scan software, there IS may still be porous to incidents of IIDTRC due to collaborative and colluded practices of employees and external agents (Gaudin, 2002). In addition, with the aid of dishonest employee/insider in the target retail company, the external agents and dubious information security experts and their accomplices could equip themselves with evolving technical tools to manipulate the systems.

Due to the techie knowledge of the employees (software engineers, IS/T administrator), they often exploit the IS weakness related to configuration, functionality or application. In the CIFAS (2011) and Verizon Risk Team Survey Report (2012), they indicated with the used of phishing (via pretexting and solicitation) as IIDTRC vector of choice, external cybercriminals relied on the personal touch with more than 78 per cent of IIDTRC cases involving in-person contact. They noted that even in the high-tech business world, all facets of cyber-crimes would not get done without an in-person 'meet and greet'. For some of these modes (e.g. social engineering and patchable software vulnerability) of carrying out IIDTRC to be successful, Verizon's Data Breach Investigations Report (DBIR) (2012) suggests that the nature of the modes have to depend on the insight provided by the insider who may have comprehensive knowledge of the targets retail companies.

In some of the IIDTRC cases, these modes could lead to advanced persistent threats (APT) techniques such as Distributed Denial of Service (DDoS), Botnets and zombies, Social Network Attacks, Clickjacking /Exploit kits/Crimepacks, Infected Near-field communication (NFC), Scareware – fake security software warnings. CSO Magazine (2011) agrees that IIDTRC those were linked to APT were perpetrated through sending internal data information to the external site/entity, tempering of the command/control channel, disabling/interfering with security control, stealing of login details, Sequel Query Language (SQL) injection and key-logging procedures and abuse of system access/privilege.

2.4.3 Targeted Assets by the Internal Identity Theft Related Crimes Perpetrators

It is imperative to for this review to discuss losses associated with personal identifiable information/data (PII/D) stolen by IIDTRC perpetrator in relation to the quantification of online retail information Systems assets/data types. The review of the losses in the context of this research was almost impossible. There was almost no report that indicated categorically the number of PID/I records compromised or lost. There were always issues of concern in relation to privacy of identity owners, mostly in relation to records containing names, e-mail address, source codes, etc. CIFAS (2013) reports survey indicated that IIDTRC incidents those involve theft of payment card information (containing names, e-mail address, source codes, etc.) are more than 48 per cent, followed by the authentication PID/I credentials with 42 per cent.

The IIDTRC do not include only the theft of customers and employees PID/I, the identity of the companies are also vulnerable. Dean *et al.*, (2011) noted that some companies' product patent and formulas are sold at the cheapest rate by the IIDTRC perpetrators. Some are sold at about 70 per cent lesser than the cost of the patented versions on the online black market. Table 7 shows the variety of compromised IS/T assets classified by those occurred in all the business (irrespective of the size) and in big business, and by PID/I name, incident and record.

Variety of Compromised PID/I	Label	All Business		Large Business	
		Incidents (%)	Records (%)	Incident (%)	Records (%)
Payment card number	CardData	48	3	33	1
Authentication PID	PIDCredit	42	1	35	1
PID (Name & Address)	Personal	4	95	27	98
Trademark, TradeSecret	OrgData	4	1	37	1
Bank Account Number	BankData	2	1	10	1
System Info. (Config &Svcs)	SysInfo	2	1	15	1
Unknown	Unkown	44	1	2	

Table 7: Variety of Compromised PID/I vs IIDTRC Incidents in Business

Adapted Verizon RISK Team Survey Report (2012)

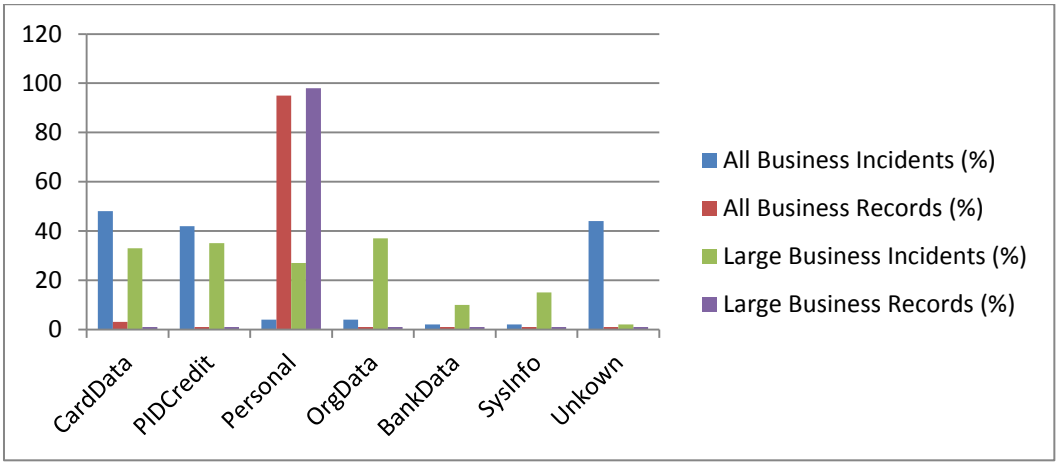


Figure 4: IIDTRC Incidents against Variety of Compromised PII/D

Figure 4 deducted from the table 7 shows chart of the targeted personal identifiable information and assets which have highest records compromised in both all and large business cases – 95 per cent and 98 per cent, though these cases are associated with 4 and 27 respectively. This indicated that the impact of IIDTRC incidents has no relationship with record compromised. In some IIDTRC cases, top business executives used their company's name to secure the fraudulent transaction.

Sometimes these incidents bring dents and insults to the company, not only financial loss. The Lloyds Bank ex-head is a typical instance (see the IIDTRC cases analyses from the banking sector in Appendix 2). In June, 2012, the former head of Lloyds' online security head (Jessica Harper) was jailed for five years for IIDTRC related to account-take-over and account withdrawals. Jessica Harper was convicted for submitting some 93 bogus invoices.

2.4.4 IIDTRC Perpetrators: Who are they and where are they?

Metropolitan Police Operation Sterling MPS (2009) reported that most employees who had been employed less than one year are more likely to collaborate with senior colleagues to commit internal identity theft related crimes (IIDTRC). CIFAS (2011) suggested that some employees use their management positions and responsibilities because of their authority and access to unlimited information systems operations. In CIFAS (2010) extensive report, it was suggested that the cases of IIDTRC can be categorised based on the operation units of some retail companies.

From the table 8 below, Retail stores, Customer Contact Centre and Field Units are among the most targeted online retail business areas for IIDTRC perpetration. This report corresponds with the Fighting Retail Crime Report (2012) which suggests that among 40 per cent of the companies interviewed; more than 25 per cent of their total IIDTRC perpetrators were supervisors, security officers and senior administrators of which 56 per cent of the perpetrators held technical positions. 75 per cent of the perpetrators were current employees and 65 per cent of these perpetrators occupied other positions with other companies.

	Years (%)	
Business Areas	2008	2009
Branch/Outlet/Store	36.62	59
Customer Contact Centre	45.77	24.33
Field Unit	10.56	8.33
Finance	-	1
IT department	0.7	0.33
Others	2.82	4.0

Table 8: IIDTRC Incidents vs Operational Department (Adapted from CIFAS, 2010)

Table 9 below which was adapted from Verizon RISK Team Survey Report (2012) shows the distribution of IIDTRC perpetrators by per cent of incidents in relation to their employment position. It shows regular employees and end-users are categories of employees that are more likely to indulge to IIDTRC because of the job roles and operations. Other examples of the regular employees include corporate end-users – call-centre employees, who take advantage of their IS access/user privileges and use them to seek cashable forms of personal identifiable data/information (PID/I) such as bank account numbers and payment card data. This report suggests that IIDTRC perpetrators need not be the super-users or most trusted of information systems users to manipulate information systems.

Job Roles of IIDTRC Perpetrator	**Percentage of IIDTRC Incidents (%)**
Regular Employee/End-User	61
Finance/Accounting	22
Executive/Upper Management	11
Helpdesk	4
System/Network Administrator	2
Unknown	1
Others	1

Table 9: IIDTRC Incidents vs Job Roles

While the accounting/finance employees are noted to indulge in IIDTRC due to their position or their accessibility to personal accounts and financial forms and records, IS administrators/developers comprises of significant per cent of the perpetrators. 'Others' in table 9 means incidents of IIDTRC indulged by business partners and outsourcing firms. Verizon RISK Team Survey Report (2012) also shows that in retail industry alone, 22 per cent of the IIDTRC are perpetrated by partners/remote, vendors, and outsourcing companies who are responsible for managing the point of sale (POS). ACFE (2014) agrees with this report suggest that most employees' fraud schemes involve the accounting department or upper management. The ACFE (2014) indicates that more than 30 per cent of fraud cases are committed by accounting department and over 20 per cent of fraud case is committed by the upper management or executive level employees. The next commonly cited are employees from the digital marketing and sales departments. Forrsight Survey Report (2013) on the distribution of employees indulgent in IIDTRC (in relation to department) agrees with Verizon RISK Team Survey Report (2012).

The Forrsight Survey Report (2013) indicated that the current employees abetting the former employees in indulging IIDTRC are on the increase. Such perpetrators often sales the online retail companies' IS/T credentials (access codes, authentication processes, de-provisioning of user accounts procedures, etc.) to the online 'black market'. The Forrsight Survey Report (2013) categorised 'likely IIDTRC perpetrators' in business organisations into four groups: Rogue which comprises of 9 per cent, HERO – the Highly Empowered, Resourceful and Operative Employees comprising of 16 per cent, Dis-enfranchised which comprises of 34 per cent and the Locked-down with 41 per cent. This Report suggests Rogue and the Locked-down which comprises of the 50 per cent of the total employees who pose the greatest IIDTRC risks.

In addition, CIFAS Report (2013) suggests the following IIDTRC perpetrators attributes: male employees aged 25, fully employed, low paid, working in junior non-management, possibly in financial difficulties and may have worked in the victim business organisation for less than a year. In the same vein, CIFAS (2011) indicated that the employees who are likely to pose major IIDTRC risks to the retail companies have common characteristics such as being male between 30 to 40 years. Table 10 below shows the gender distribution of the IIDTRC perpetrator in percentage increment from 2008 to 2009.

	Age distribution (Total)		**Men**		**Women**	
Forms of IIDTRC	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**
Account Identity fraud	32	30	31	32	34	29
Disclosure of business data	40	27	40	27	39	27
Disclosure of Personal data	26	26	28	27	23	25

Table 10: Age and Gender Distribution of IIDTRC Perpetrators

(Adapted from CIFAS, 2011)

CIFAS (2013) agrees with CIFAS (11) and adds that theft of intellectual properties which comprise 78 per cent to 92 per cent of the overall IIDTRC cases/incidents were perpetrated by male employees. This report corresponds with FraudTrack (2012) report that IIDTRC cases are dominated by the male employees with women are being linked to 18 per cent of reported cases of theft of intellectual properties. Kroll Consulting Annual Global Report (2010) indicated that 48 per cent of companies in the UK are victims of internal identity theft related crimes (IIDTRC) with retail sector as one of the companies on high risk.

The impact of IIDTRC on businesses is summarised in the figure 11 below with retail sector, financial services, the professional services and telecoms topped the list.

Chart 2. Percentage of companies within industry reporting information theft, loss or attack

	2010	2009
Financial services	42%	24%
Professional services	40%	27%
Technology, media and telecoms	37%	29%
Retail wholesale and distribution	26%	19%
Consumer goods	25%	22%
Natural resources	22%	27%
Construction, engineering and infrastructure	21%	23%
Healthcare, pharmaceuticals and biotechnology	19%	21%
Travel, leisure and transportation	18%	23%
Manufacturing	13%	23%

Table 11: Percentage of Reported IIDTRC within Industries

(Kroll & Global Fraud Report, 2010)

In addition, the CIFAS: The UK's Fraud Prevention Service, (2013) noted that there is prevalent of the cases of IIDTRC in the busy cities in UK compared to less busy ones. This is perhaps because of the siting of most companies in the major cities; London and Glasgow top the chart as show in table 12 below.

Business Area	**Cases of Internal employee fraud (%)**
London	22.91
Glasgow	8.33
Sheffied	6.25
Leeds	4.17
Ipswich	4.17
Peterbourough	4.17
Portsmouth	4.17
Bradford	2.08
Bolton	2.08

Table 12: IIDTRC Cases across UK Cities (Adapted: CIFAS, 2013)

2.4.5 Internal Identity Theft Related Crimes: The Resulting Practices

In most the IIDTRC incidents, the perpetrators used the stolen assets for financial gain. In other cases, they use the stolen assets to create bank account or apply for the fraudulent loan or sell the data to the black market. CIFAS Report (2010), in comparing the trends of IIDTRC from 2008 and 2009, indicated that fraudulent account withdrawals, account disclosure have become common practices of the IIDTRC. Figure 5 below shows an increase of incident of account withdrawal in the victim companies within two years 2008 and 2009.

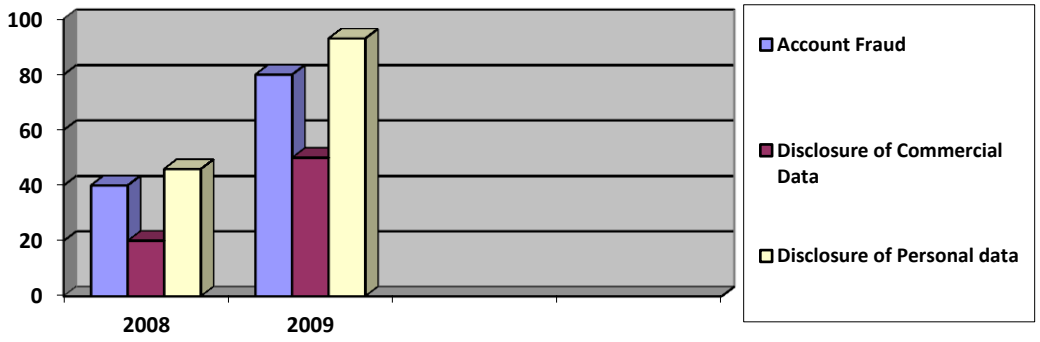


Figure 5: Trends of Account Withdrawal Incidents between 2008 and 2009

Adapted from CIFAS (2010)

CIFAS Report (2012) indicated that there is almost 50 per cent rise in the number of cases of IIDTRC compared to the previous years; which account for as much as 80 per cent of all computer and internet related crimes. In line with CIFAS (2012), Dean *et al.,* (2012) noted that IIDTRC increase approximately by 30 per cent from 2011 to 2012; and CSO Magazine also indicated that IIDTRC rose from 55 per cent to 60 in a one-year period.

Fraudulent Account Withdrawals: The Fraudulent Account Withdrawals involve unauthorised access or manipulation on a customer account information details for personal benefit. CIFAS Report (2010) suggested that fraudulent account withdrawal has increased drastically from 2008 to 2009. Other practices linked with Fraudulent Account Withdrawals are fraudulent account transfer to the employee account and fraudulent account transfer to the third party. Table 13 below shows the increment in per cent of forms of fraudulent account withdrawals.

	2008 (%)		**2009 (%)**		
Account Withdrawals	**Cases**	**Total**	**Cases**	**Total**	**Changes**
Fraudulent account transfer to 3rd party	5	38	14	31	180
Fraudulent account transfer	5	38	9	20	80
Fraudulent account withdrawal	3	23	22	47	633

Table 13: Incidents of Fraudulent Account Withdrawal between 2008 and 2009

(Adapted from CIFAS, 2010)

Disclosure of Commercial or Personal data: This involves the use of commercial or business identity's data without the consent of the data owner. The use of these data for unauthorised purposes always places the victim companies and individuals at an operational risk and financial difficulties respectively. This is the case of the employee colluding with organised criminals into compromising the customer data and information. The criminals could use the data to plunder the victim's account by making multiple applications in their names.

CIFAS (2010) suggests that intelligence from law enforcement agencies noted infiltration of organised criminal groups in businesses are responsible for disclosure of commercial and personal data. Table 14 below shows the trends of the cases of the data disclosure practices between 2008 and 2009.

	2008 (%)		2009 (%)		
Data Disclosure	Cases	Total	Cases	Total	Change
Disclosure to third party	11	50	20	55.6	45
Personal use of data	6	27.3	5	13.9	-20
Alteration of data	1	4.6	2	5.6	50
Change of payment rules	1	4.6	1	2.78	0

Table 14: Data Disclosure Incidents between 2008 and 2009

(Adapted CIFAS: UK's staff Fraud Landscape, 2010)

In summary of the common forms of fraud practices related internal identity theft crimes, the UK Fraud Advisory Panel (2011) classified common types of identity theft related crimes into two categories Personal Identity Crime and Corporate Identity Crime.

Table 15 below summarises the common respective types/schemes of the Personal Identity Crime and Corporate Identity Crimes.

Category of IIDTRC	Common types and schemes
Corporate identity theft related crimes The impersonation of another company for financial or commercial gain. Fraudsters steal a company's identity and/or financial information and use it to purchase goods and services, obtain information or access facilities in your company's name.	**Company hijacking:** A fraudster submits false documents to a retail companies to change the registered address of their employer company and/or appoint 'rogue' directors. Goods and services are then purchased on credit, through a reactivated dormant supplier account, but they are never paid for. **Company Impersonation:** A fraudster impersonates a retail company (sometimes by purporting to be a director or key employee) to trick customers and suppliers into providing personal or sensitive information which is then used to defraud the retail company. In some cases, the retail companies may be impersonated using phishing emails, bogus websites and/or false invoices.
'**Personal Identity Crime'** is commonly used to describe the impersonation of another person for financial gain. Personal identity criminals steal your personal identity and/or financial information and use it to purchase goods and services or access facilities in someone's name. This scheme is use of a false identity or another person's identity to obtain goods, money or services by deception. This often involves the use of stolen, counterfeit or forged documents such as passports, driving licences and credit cards.	**Application Fraud/Account Takeover:** A fraudster applies for financial services (e.g. new credit cards or bank accounts) using individual's name or changes the individual's postal address. Impersonation of the deceased: A fraudster uses the identity of a deceased person to obtain goods and/or services. **Phishing:** A fraudster sends an email to an individual claiming to be from his or her bank or other legitimate online business (e.g. a shop or auction website) asking the individual to update or confirm his or her personal or financial information such as password and account details. This information is then used to impersonate the targeted individual and gain access to accounts. **Present (Current) Address Fraud:** A fraudster living at your address (e.g. a family member) or nearby (e.g. a person living in the same block of flats) uses your name to purchase goods and/or services and intercepts the mail when it arrives.

Table 15: Respective Types/Schemes of Personal and Corporate Identity Theft Related Crimes

The UK Fraud Advisory Panel (2011) suggests that the category and types of IIDTRC depend on the various intentions of the perpetrators. Some of the intentions are deliberate with malicious intent; inappropriate and not a malicious intent, and unintentional without malice. The Verizon DBIR (2013) agrees with the UK Fraud Advisory Panel (2011) and indicated that 93 per cent of IIDTRC were linked to deliberate malicious activity. This report noted that some inter-connected intentions drive 'the inappropriate' and not malicious intent, and unintentional without malice. Under the category of those perpetrators with malicious intention, three-quarters of them had authorised access to the information stolen, with approximately 19 per cent of the cases involved either collusion or collaboration with outside accomplices.

In contrast, the CIFAS Report (2011) posits different intentions of the IIDTRC perpetrators. It suggests that 35 per cent of the IIDTRC perpetrators stole from their employers to gain new job, of which in 25 per cent of these perpetrators gave the stolen assets to the new companies. IdentityForce (2014) agrees with CIFAS Report (2011) and suggests that in every 25 per cent of the IIDTRC cases, the perpetrators were actively recruited by someone outside the targeted company, of which 65 per cent of these perpetrators were coerced at their workplace, 15 per cent are coerced remotely while accessing their employers' networks from their homes or other location; while more than 25 per cent of the coercion location remained unknown.

2.5 Internal Identity Theft Related Crimes Prevention

This section discusses the strategies recommended by the renowned Information Systems or Techology (IS/T) Security consulting firms' studies (e.g. Global Information Assurance and Data Security Essentials (GIA_DSE). The three firms discussed in this section includes but no limited to Global Information Assurance and Data Security Essentials (GIA_DSE) and Forrester Seeburger Security (FSS) Consortium for Cyber Security Action (CCA). These firms suggest practical solutions on how to mitigate internal identity theft related crimes in online retail.

2.5.1 Recommendations for Prevention of Internal Identity Theft Related Crimes

Vulnerabilities and Patch Management is among the top five security strategies recommended by the IS security consulting firms, emphasizing the importance of vulnerability testing in the prevention of IIDTRC. It was ranked second in the column of the FSS, third in the GIA_DSE and fourth in the CCA.

These consulting firms recommend that retail companies should ensure that vulnerability and patch management of security software is maintained and updated. This suggests that vulnerabilities management is an essential data security tools and the maintenance should be the core statistic of a security metrics for any business IS security. Along with the vulnerability management, code and configuration reviews were suggested as elements that need to be given priority in patch and vulnerability management. Other security strategies that are suggested by the firms are Application and Data Security, Threat Identification focused on Internal Human Threats Controlled Access Based on the Need to Know and User security Training and Awareness. This suggests that these strategies reduce IIDTRC risks across the retail business operation.

However, The User security training and awareness (10) in FSS, Threat Identification focused on Internal Human Threats (2) in CCA, and Controlled Access Based on the Need to Know (15) in GIA_DSE, shows disparity in the level of priority given to the end-user and human roles by these firms. Critical analysis of the security strategies recommended by the FSS and GIA_DSE shows that they integrated both the situational-based and offender-based approach, while CCA focuses more on situational-based IIDTRC mitigation.

In addition, the CCA recommendation is similar to Microsoft's Enhanced Mitigation Experience Toolkit (EMET) which focuses on finding specific IIDTRC vulnerabilities and blocks potential security exploits (TechNet Blogs, 2013). SANS Critical Security Controls (2008) suggests that conventional IIDTRC prevention based on data security certainly have their place, although the success of the IIDTRC prevention strategies depends mostly on how the IS security management implement them.

Other recommendation such as Kill-chain approach (KCA) by Lockheed and Hutchin (2010) essentially requires the integration of both technology and human roles mitigation approaches, with much emphasis on the implementation for KCA success.

Table 16 and table 17 summarises the list of the internal identity theft related crimes (IIDTRC) prevention strategies recommended by the top IS/T Security companies.

Forrester Seeburger (2013) suggests that the following initiatives are recommended to be the companies' top IT security priority in the prevention of IIDTRC. They are arranged in the decreasing order of how the priority should be given by the companies.

Priority	FSS	CCA	GIA_DSE
1	Data Security	Inventory of Authorised and Unauthorised Devices	System Characterisation and defining the scope and boundaries IS
2	Managing Vulnerability and threats	Inventory of Authorised and Unauthorised Software	Threat Identification focused on Internal Human Threats
3	Business continuity/disaster recovery	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Vulnerability Identification in Information Systems
4	Managing information risk	Continuous Vulnerability Assessment and Remediation	Control Analysis and Review of Data Security Controls
5	Application security	Malware Defences	Likelihood Determination of possible Exploit/Vulnerability
6	Aligning IT Security with the business	Application Software Security	Impact Analysis
7	Regulatory Compliance	Wireless Device Control	Risk Determination of Exposure to IIDTRC (low, medium, high)
8	Cutting Costs and /or increasing efficiency	Data Recovery Capability	Results Documentation and Process Presentation
9	Identity and access management	Security Skills Assessment and Appropriate Training to Fill Gaps	Data Security Control Recommendations
10	User security training and awareness	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	

Table 16: Recommended IDTRC Prevention Strategies by GIA_DSE and FSS

Adapted from Global Information Assurance and Data Security Essentials (GIA_DSE), (2012) and Forrester Seeburger Security (FSS), 2013)

Priority	FFS	CCA
11	Complying with security requirement placed upon business by their partners	Limitations and Control of Network Ports, Protocols, and Services
12	Complementing the business security required with business partners/third parties	Controlled Use of Administrative Privileges
13	Integrate physical and logical security	Boundary Defence
14	e-Discovery	Maintenance, Monitoring, and Analysis of Security Audit Logs
15	Security outsourcing	Controlled Access Based on the Need to Know
16	Engaging the law enforcement agencies	Account Monitoring and Control:
17		Data Loss Prevention
18		Incident Response and Management
19		Secure Network Engineering
20		Penetration Test

Table 17: Recommended Identity Theft Related Crimes Prevention Strategies by CCA and FSS (Adapted from Consortium for Cybersecurity Action (2012) and Forrester Seeburger Security (2013))

2.5.2. Practices of Internal Identity Theft Related Crimes Prevention

Wang, Yuan and Archer, (2006) and Adams (2008) agree that there is a need for research to look into the internal identity theft prevention practices in a particular business sector. A few studies (e.g. Schulze and Shah, 2009; Elliot and Willingham, 2001; Calder and Watkins, 2005) adhere to this suggestion. Schulze and Shah (2009) suggest that conducting information process risk assessment and training of employees to recognise bogus online applications (credit card, bank account) in the online retailing have proven to be good security strategies in preventing IIDTRC. Elliot and Willingham (2001) also agree that companies that adhere to the practices effective data protection and compliance management often succeed in preventing IIDTRC cases in their organisations.

UK Data Protection Act 1984 and 1998 provides the guidelines for the IIDTRC prevention which include effective protection of customer's data, employees' recruitment process and secure record management, effective monitoring of the employees and structured training of employees on IIDTRC awareness. However, Gayer (2003) and Calder and Watkins (2005) argue that any guidelines for prevention of IIDTRC is reliant on the readiness of retail management to effectively implement the suggestions. The following sections summarises IIDTRC prevention practices, although not the exhaustive lists of the practices.

2.5.2.1 Collins Key Business Asset Security

Collins (2003) suggests that an effective security of the key business assets: people, processes, property and proprietary information, enhances effective prevention of internal identity theft-related crimes in business organisations.

People: Security of Employees

CIFAS (2013) agrees with Collins (2013) and suggests that employees' awareness of IIDTRC perpetration mechanisms – collusion, coercion and collaboration, as one of the most effective practices for prevention of IIDTRC. Hinds (2007) noted that good reporting procedure for IIDTRC incidents re-builds employees confident that the IIDTRC cases would be handled according to the business ethics of their organisation. CIFAS (2011; 2013) and Hinds (2007) agree that Vetting and Screening of Employees, Staff Monitoring, and Staff Profiling are the three proven IIDTRC prevention practices.

***Vetting and Screening of Employees:* -** Hinds (2007) suggests that background screening is a first line of security in the prevention of IIDTRC. Effective screening reduces the risks associated with business organisations employing potential fraudulent employees. CIFAS (2011) – 'Enemy Within' suggests that lack of checks and controls of employee recruitments increases the risks of employing dishonest employees that may pose IIDTRC risks. The CIFAS (2013) argues that the recruitments checks and controls do not only identify the fraudulent staff vulnerable to internal identity frauds but also prevent the infiltration of the employees alike. Fraud Advisory Panel (2011) reports that the majority of potential employees lie in their job applications.In their report, it was indicated that 25 per cent of the curriculum vitae of the applicants examined were falsified with information related to academic qualifications and employment histories to secure their potential employment.

This report also recorded that 34 per cent of managers failed to check the background of their prospective employees. Of all companies that were surveyed by the Chartered Institute of Personnel Development (CIPD) cited in Hinds (2007), only 77 per cent of the companies cross check their potential candidate references. One may argue that the remaining 23 per cent is smaller compared to the 77 per cent, but this could do much more damage to any organisation considering the impact of IIDTRC. These findings suggest the relented effort of personnel managers in vetting processes in many retail companies. If the fight against internal identity fraud related crimes is ever going to succeed, there is a need for prospective employers to ensure the credible vetting of all new employees.

Staff Monitoring: This involves the monitoring of employees through human resources (HR) and promotion of the internal corporate culture of employees. Hinds (2007) suggested that companies with a good tradition of internal HR management have lesser cases of internal frauds compared to those without. Many companies invest a lot of resources to secure their IT infrastructure from external attack sources like hackers but neglect the threat posed by the dishonest employees. Basel Committee on Banking Supervision (BSBS) (2012) agrees with Hinds (2007) and suggests that HR management promotes effective monitoring of the employees who are living a suspicious lifestyle that may pose potential threats to the business. Dean *et al*., (2012) agree with BSBS (2012) and suggest that HR managers could create a desired culture in every organisation by promoting: fraud management policy, employee fraud prevention policy, code of conduct or business ethics, disciplinary policy, fraud reporting policy, whistle blowing policy, staff assistance policy and fraud specialist policy. ACAS (2008) also advised business organisations to set standards of performance and conducts which should be monitored by company rules. Although, legal action against the fraudster based on the business policy might be expensive, but it still serves as deterrence for susceptible IIDTRC perpetrators and their collaborators.

Staff Profiling*:* This is a technique of developing a behavioural pattern of IIDTRC suspect who has not been caught yet. Hurst (2010) suggests that profiling often encourages thorough investigation, effective risk analysis and paves a way for a possible change of information security strategies and amendment of policies to discourage crimes within organisations. Profiling helps businesses to establish which job roles or business areas pose the greatest threats and are most vulnerable to the risks of IIDTRC. In addition, profiling helps to find out geographical hot spots of IIDTRC and enable the intelligence services to design predictive modelling to prevent potential IIDTRC.

Security of Process, Property and Proprietary Information Security

Financial Crime and Service Authority (FCSA) (2009) suggests that online retail companies should invest more in security systems and internal data controls to avoid being targeted as the weakest link. The advancement of the information technology has enabled the IIDTRC perpetrators to continue to refine and update their techniques. For instance, the recent 2011 Sony PlayStation Network (PSN) attack remained a lesson for the business organisation that thorough and updated proprietary information security is indispensable for internal data security. If PSN was thoroughly subjected to internal data and proprietary security and other rigorous intrusion detection control tests, perhaps, the compromise of the about 70 million user's personal identifiable information would have been averted. Though, there is still no tip for the cause of the PSN attack linked to the dishonest act within the company, the message for the need of effective internal data proprietary security monitoring remains obvious. Dean *et al.,* (2011) reported in Ponemon Institute Research that 28 per cent of the IIDTRC cases in 583 US companies occurred among the mobile workforce, of which 44 per cent of the companies surveyed still view their IT infrastructure as relatively insecure, while 90 per cent have had cases of IIDTRC at least once in prior 12 months. This report shows that some of the online business organisations including retail companies allow their employees to store valuable customer's personal identifiable information on online applications such as Google Dropbox and Docs.

Verizon DBIR (2012) agrees with Dean *et al.,* (2011) and indicates that out of 447 business organisations that participated in their survey of how employers use social media in their business, 52 per cent of small businesses depend on social networking sites, with only 8 per cent of the small businesses monitor what staff posted on those sites. These business practices expose the data to theft and make the customer's PID/I vulnerable to IIDTRC. In some cases the use of the social networking sites – LinkedIn, Twitter, Facebook, leaves the digital trails that make online companies susceptible to social engineering. These related crimes are still rampant because of the security loopholes of the IT/IS infrastructures and proprietary systems. However, some of the new complex technologies that have been noted to have proven security for process, property and proprietary information security are biometric technologies, cryptography, authentication and certification and single-sign-on technologies (Schneier, 2004). Though, some of these leading data security technology solutions – IBM AppScan, forensic data warehousing, Vontu by Symantec, exist, companies might not make much out of these security tools if there is no effective security audit and compliance management (IBM Software, 2012).

2.5.2.2 The US National Strategy for Identity Theft Prevention

This strategy was developed to support federal, state and local law enforcement agencies for prevention of identity theft crimes and was recommended to be adopted in the U.S business organisations. The main seven components of the US national strategy are information protection, legislation, partnerships and collaboration, public awareness, reporting procedures, training, and victim assistance. It is vital to emphasise on the three key components: Legislation, Partnership and Collaboration and Training, because they extend the understanding of the IIDTRC prevention suggested by Collins (2003) and because of the suggested impacts these practices have on IIDTRC prevention (McDonald *et al.*, 2006). Table 18 summarises the four components US National Strategy for Identity Theft Prevention.

Strategy	**Features and Impact on IIDTRC prevention**
Partnership and Collaboration	Strategy for effective IIDTRC prevention has been adopted in many business organisations in the following instances; Indiana State Police for the US Strategic Alliances, Computer and IT and National White Collar Crime Centre (NW3C), 'Tiered Approach' among students and IS/T security experts, Scientific Working Group on Digital Evidence (SWDGE), the Nigeria's Police Economic and Financial Crimes Commission ("EFCC"), the UK's Central Sponsor of Information Assurance and Office of Cyber Security Office and Cyber Security and Information Assurance (OSCIA), the UK's anti-fraud scheme – TRADE (Transactis Risk Assessment Data Exchange) which shares transactional data to enable the detection of potential IIDTRC and computer related criminals and fraudsters in business organisations, the Defence Advanced Research Projects Agency (DARPA).These collaborated bodies work with an aim to establish standards practices to guide professionals in investigating identity theft crimes and other computer related crimes. They work together, sharing their expertise, both in areas of provision of digital investigatory strategies and evidence, to foster the security threats of businesses. Rosenberg (2010) suggests that partnership approach which is used in biological and nuclear arm controls treaties could help prevent identity theft crimes and encourage robust practices in investigating these crimes across nations, business organisations, industries and sectors.

Strategy	Features and Impact on IIDTRC prevention
Legislation	The harmonisation of the data privacy and security legislations across businesses can reduce the bottlenecks during IIDTRC reporting. Bringing together of various cross-border data protection policies provide the opportunity for thorough investigation of IIDTRC in the emerging business networking and outsourcing. Sommer (2012) suggests that harmonised policy approaches in IIDTRC prevention at an international level is an indispensable practice that have been pioneered by US governments.
Legislation	Sommer (2012) further suggests that comprehensive legislation on identity theft prevention would help to tackle the challenges related to 'the admissibility' of electronic evidence and other related legal hurdles. Breyer (2012) agrees with Sommer (2012) and suggests (in the Reference Manual on Scientific Evidence) that law seeks decisions that fall within the boundaries of scientifically sound knowledge, but it is sometimes difficult to achieve in practice if there is no existing policy on crimes prevention to support provision of the scientific evidence.
Training	A continuous training for the online retail staffers helps to match the evolution of the Information Systems. An anonymous New Jersey Regional Computer Forensics Laboratory (NJRCFL) director and FBI supervisory special agent noted the importance of staff training. He said that being an IT/S security expert in IIDTRC prevention is 'not only what I know, but what I know that is not so' (Mercuri, 2005). Wilkinson and Haagman (2011) suggest that the computer security experts have overall responsibility to be updated with practices of the IIDTRC prevention. The G8 on standards for the Exchange of Digital Evidence also emphasised the need for training in prevention of IIDTRC. Researchers (e.g. Walker, 2006; Meyers and Rogers, 2004) agrees with G8 and suggest that since there are certification for fraud investigators in other fields (accounting, finance, and banking), the needs for the certified professional examinations for identity theft crimes in computer crimes should be given a due consideration.

Table 18: US National Strategies for Identity Theft Related Crimes Prevention

2.5.2.3 Use of Information System Governance and Security Intelligence

Conte (2003) in the 'Global Information Assurance Certification' suggests the following IIDTRC prevention practices: IS/T monitoring and CCTV and Network Intrusion Detection Systems; System Characterisation; and IIDTRC Incidents Results Documentation. These steps, he noted, could improve the control analysis to address the identified IIDTRC and detect the likelihood that a privilege user or a dishonest employee may exploit a known vulnerability. Conte suggests that an application of the control analyses reduces the risk of the insider threat to system vulnerability and that the control tools such as DirectoryAlert and ServerAlert by NetVision can reduce potential IIDTRC threats.

Forrester and Seeburger (2013) agree with Conte (2003) and suggest three key elements: Define Your Data, Dissect Your Data, and Defend Your Data, for effective internal data security intelligence against IIDTRC. Dissection of the data is the processes of critical data analytics for security intelligence. It can be defined with an acronym: INTEL – Information, Notification, Threats, Evaluation and Leadership. With an efficient data definition and data dissection in place, these principles would enhance the security against IIDTRC.

In addition, efficient implementation of these practical elements could reduce data leakages by encouraging the principle of least privilege – strictly enforce access control, inspect data usage patterns to identify abuse, dispose of data when no longer needed and encrypt data to limit the access. Forrester and Seeburger (2013) further suggest that data with defined location and index would facilitate the development of a life cycle for data classification, cataloguing and data discovery to reduce the risks of the IIDTRC.

2.5.2.4 The Use of the Information Security Audit (ISA)

Dean *et al.,* (2012) suggest that companies should utilise three lines of defence – data security, privacy controls and practices, with IS security audit playing the critical role in implementing these lines of defence. Association of Certified Fraud Examiners (ACFE) (2014) Report on the Nations Occupational Fraud and Abuse agree with Dean *et al.,* (2012) and suggests that since 2002 IS security audit has consistently proven to be more likely to prevent identity theft related crimes than other prevention practices.

Several researchers (e.g. Hooks and Kaplan and Schultz, 1994; Steinnon, 2006) agree that information security audit plays a substantial role in IS security (ISA) management. Dooley (2009) suggested that business owners must make a substantial investment on ISA to protect consumer's PII/D from the emerging social and technological oriented IIDTRC threats. Wells (2010) agrees with Dooley (2009) and remarked that half the combined cost of IIDTRC and detection could be the cost of their prevention through effective ISA. Hua and Bapna (2012) has suggested that countries should prioritise practical and strategic IS security checks to avert data leakages which originate from the inside business organisations.

Some companies have adhered to the suggestions on the importance of ISA in the prevention of IIDTRC. Dean *et al*., (2012) noted that the International Data Corporation (IDC) survey conducted in 2007 found that companies across industries spent more than 19 per cent of their IT budgets on ISA. The PWC's ISBS (2014) reports that 50 per cent of UK companies plan to spend more on IT security with an increase of 9 per cent more in 2012 than the previous year. This report also indicated that the UK Cyber security Operations Centre spends more than £5 million annually on information security issues while the US federal agencies budgeted about $6.5 billion on data security assurance alone for the fiscal year 2012. In agreement with Dean *et al*., (2012), the PWC[6]'s ISBS[7] Report (2014) on the strategies for identifying IIDTRC risks in the business organisations noted that ISA was rated at 75 per cent while other strategies such as IS break-down and loss of company assets account for 25 per cent. In addition, ACFE[8] (2014) suggested that more than 43 per cent of IIDTRC incidents were detected by use of the ISA of which 7 per cent was detected by the independent external security auditing. This report shows that more than 50 per cent of such crimes could be detected by effective Information Systems security audit.

2.5.2.5 Detection Mechanisms as Identity Theft Prevention Practice

Understanding some of the key detection mechanisms available at the disposal of the internal identity theft related crimes (IIDTRC) victim would guide the understanding of some elements required for designing effective IIDTRC prevention framework. It would enable the victim to make a decision on resource allocation and the implementation-know-how in applying them and when to.

[6] PricewaterhouseCoopers: A multinational professional services firm.
[7] Information Security Breaches Survey
[8] Association of Certified Fraud Examiners

Several Research reports (e.g. ISACA, 2010; British Retail Consortium (BRC) Crime and Loss Prevention, 2011; Cichonski *et al*., 2012 and Verizon DBIR, 2013) have agreed that detecting internal identity theft related crimes incidents at the earlier moment of the incidents was escalated have least amount of repercussion, though, not lesser than if they were prevented. These reports noted that IS/T security controls are neither absolute detection mechanism as they have their downsides – cost, complexity and implementation. In addition, these reports emphases the importance of understanding the timeline of the IIDTRC incident in relation to the detection. Understanding the time frame for IIDTRC incident could increase the ability to provide comprehensive framework and capability evaluation. The timespan/line for IIDTRC incidents depends on a variety of factors and incidents detection processes.

The Verizon's (2014) Data Breach Investigation Report (DBIR) categorised the timeline analysis of IIDTRC incidents into 3 phases: pre-IIDTRC incident, active-IIDTRC incident and post-IIDTRC incident, which are aligned with IIDTRC incident detection process. The pre-IIDTRC incident is the initial phase of an incident which depicts time from the first action taken against the victim by the perpetrator until the time IS/T property is affected. This is common with network resources intrusions and point of sale (POS) abetted hacks. According to the Verizon's (2013) DBIR Report, 85 per cent of the IIDTRC incidents under this phase occurred within minutes or less.

The time for the pre-incident depends on the complexity of security platform of the victim companies. BRC Crime and Loss Prevention Report (2011) indicates that large retail companies have lesser pre-IIDTRC incident time than smaller companies because of the complexities associated with managing large IS/T infrastructure and detecting crimes in large retail companies.Active-IIDTRC incident phase covers the timespan from the pre-IIDTRC incident phase to the time when PID/I is first removed from the victims' IS/T control environment. In average, the time for this incident phase is longer – the time it takes the perpetrator to explore the network, locate and exploit the relevant IS/T platforms and then exfiltrate/collect the asset.

Cichonski *et al*., (2012) suggest in the Computer Security Incident Handling Guide (CSIHG) that abetted SQL injection-related incidents fall into active-IIDTRC incident phase and that are common in both small and bigger retail companies.

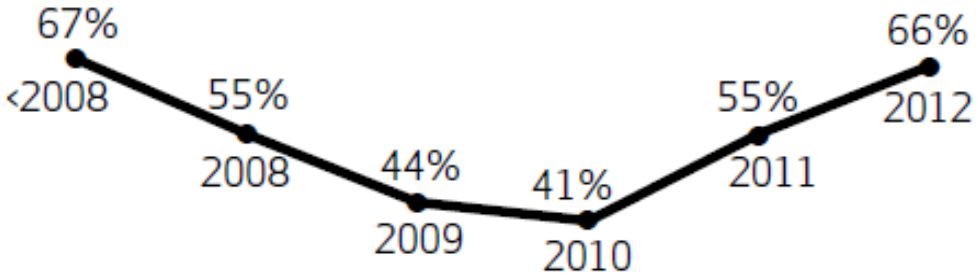


Figure 6: Trends of Undiscovered IIDTRC Incidents

(Adapted from Cichonski *et al*., 2012 cit. Computer Security Incident Handling Guide)

Post-IIDTRC phase describes the time from the active-incident phase to the time the victim discovers the incident. Figure 6 shows the distribution of IIDTRC incidents that remain undiscovered for months from 2008 to 2012. The post-IIDTRC phase may cover as much as months. Some cases took up to years since the perpetrators often cover their trails especially the incidents that are perpetrated by software engineer/administrators. This phase could extend to as much the time it takes the victim to detect or to discover the security breach, which sometimes prove impossible. ISACA (2010) indicated that 70 per cent of the post-IIDTRC phase incidents were discovered by the external parties (e.g. notification by an informant/customer, law enforcement, competing organisations, Internet Service Providers). This report suggests that the internal detection capability is lacking in most victim companies, with a few of non-technical employees discovering only 11 per cent of the incidents. Though, this analysis could be somewhat based on the size of the retail companies.

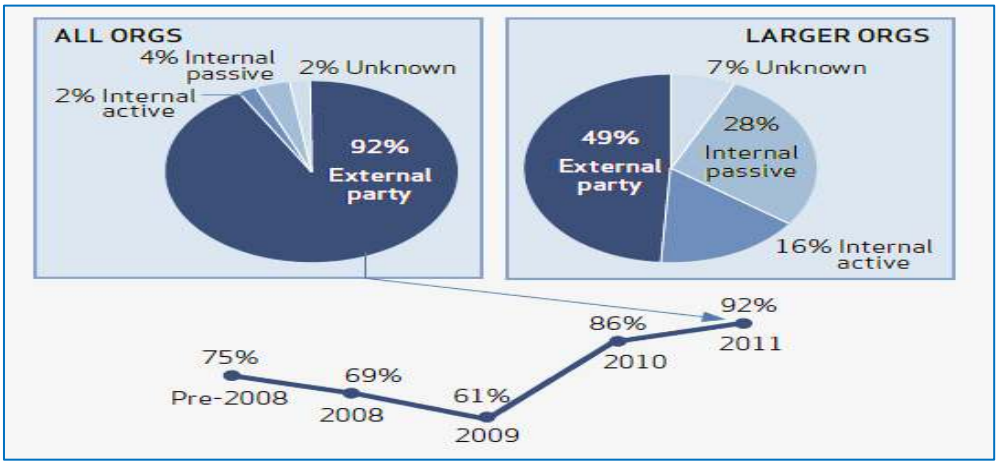


Figure 7: Detection Methods for IIDTRC in Business Organisations

(Adapted from Verizon DBIR, 2012)

Verizon DBIR (2012) agrees with ISACA (2010) and indicates, as shown in the figure 8 that from 2009 to 2011 more than 50 per cent of the IIDTRC incidents experienced by the larger companies were detected by the external party; while in aggregate, irrespective of the size, 92 per cent of these known incidents were detected by the same external party. The larger companies recorded only 16 per cent of the active detection by the internal party and only 2 per cent of internal detection was recorded in all the organisations studied. But in all, the external party still maintains the larger chunk as the source of the IIDTRC incidents detection.

In line with the Verizon DBIR (2012) Report, Verizon DBIR (2013) as shown in figure 8 suggests that few technical methods could be used to detect IIDTRC incidents. The reports agrees that end-users activities as the most effective mean of detecting IIDTRC incidents. The end-users detects and IIDTRC incidents such suspicious e-mail and slow system performance in the course of their daily responsibilities. Other common internal methods include fraud financial audit, log review, IT audit, and incident response.

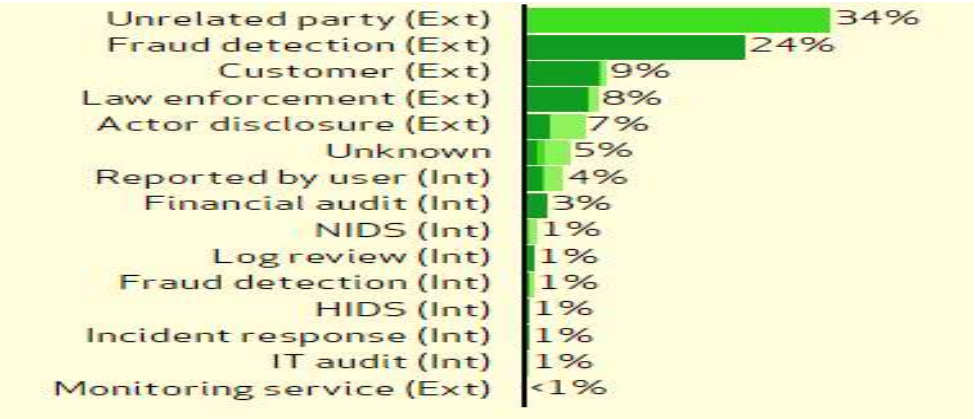


Figure 8: Methods of Detecting Internal Identity Theft Related Crimes (Percentages)

(Adapted from Verizon's DBIR, 2013)

Figure 9 below shows the table matrix plots of IIDTRC detection methods against timespans observed in 2012 by Cichonski *et al*., (2012) in Computer Security Incident Handling Guide (CSIHG). It shows that it takes 15 months for the fraud detection and 9 months for the law enforcement compared to less than 6 months recorded for the same incidents to have been detected by the internal party. There could various reasons attributed to these delays in detecting the IIDTRC cases. In some cases, depending on the nature of the business operation, the victim companies might have contingency plans in place to manage the disruption while the investigation would be carried out.

Another reason attributed to the delays associated with detecting the IIDTRC incidents is that more than 78 per cent of the incidents committed during the working hours. In some cases, more than 50 per cent of IIDTRC were detected months after the departure of the perpetrators from the victim companies.

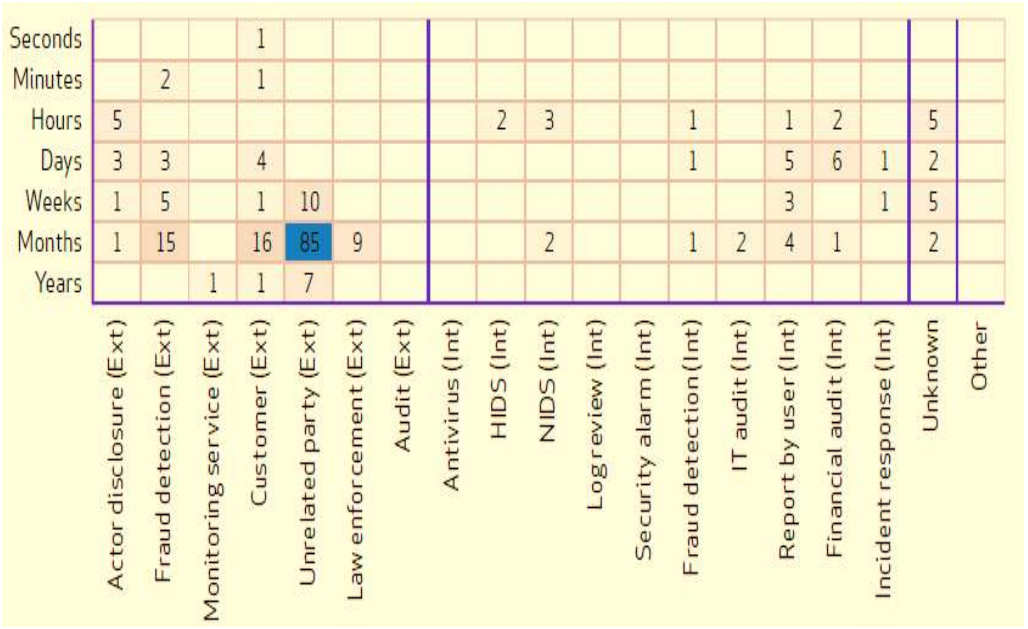


Figure 9: IIDTRC Detection Methods (Time Span)

In summary of the answers to the research questions this section has provided, table19 depicts the key IIDTRC perpetration modes in relation to their respective prevention and detection strategies. The IIDTRC prevention recommendations in section 2.5.2 indicate that retail companies should implement the recommendations which might be practicable in relation their various sizes and business processes. Even with a well-modelled IIDTRC prevention framework established by a consortium of security professionals, there is no one-size-fits-all solution. The application and implementation of the framework across business operation will differ depending on budget, business need, and process and size.

In search of the evidence-based IIDTRC prevention framework, next section explores framework available for prevention of IIDTRC in the retail companies, to investigate how these IIDTRC prevention controls at their disposal fit the business operations and processes. In addition, next section extends to answer the questions related to potential IIDTRC prevention practices and data security implementation issues that face the Information Systems management.

Mechanisms	IIDTRC Detection	IIDTRC Prevention
Infiltrated hacking: access to protect IS with stolen credential.	Monitoring of administrative/privilege activity: logon time, anomalies, malware on the system	Controlled authentication: two faction, internet protocol blacklisting, internal restricted administrative connection.
Abetted botnet and infiltration.	Registry monitoring and examination of the active system processes.	Integrity control mechanisms, Egress filtering via ports and protocols, host intrusion detection systems (IDS), updating firewalls and software security.
Tampering and copying of PID/I	Some scratches on the IS device, Bluetooth signals.	Employees training, Consistent inspection, policy implementation, anti-tampering tools – tamper switch, epoxy electronics.
Social engineering and manipulation	Call logs, e-mail logs, unusual communication, bypass of technological alerting mechanisms, visitors' log.	Clearly defined policies and procedures, general security awareness training.
Collusion and employees abetted cybercrimes	Routine monitoring of the databases, webserver, IDS and intrusion prevention systems (IPS)	Principles of least privilege account management, input validation and whitelisting techniques
Collaboration with external agents	Last logon banner, end-user behavioural analysis, logon source location analysis	Disabling default account, scanning of passwords, password-change rotation principle, sharing of the administrative duties.
SQL via back-end databases	Desk calls for account lockouts, sequential guessing and log in attempts failures.	Password policy, password throttling and effective access control mechanisms.

Table 19: IIDTRC Mode_Detection_Prevention

2.5.3 Lessons from the IIDTRC Prevention Practices

The internal identity theft related crimes (IIDTRC) prevention practices discussed above encompass the detailed guidance on protection of customer's data, recruiting employees, managing records, and monitoring the employees. PriceWaterCoopers' (PWC) (2014) suggests that even though more than 50 per cent of UK companies have adopted these practices and plan to spend more on IT security, 67 per cent of the companies expect a rise of the IIDTRC incidents. One might be deemed to ask why are the IIDTRC prevention practices discussed above arguably do not contribute to effective prevention of the crimes incidents. Vaca (2003) argues that some online retail companies that seem to comply with the IIDTRC prevention practices do have the capacity to provide effective and efficient strategies that ensure quality requirements and cost reduction. Several studies (e.g. Popa and Doinea, 2007; Dean *et al*., 2012; Forrester and Seeburger, 2013; PriceWaterCoopers' (PWC), 2014) agree that many online retail companies attributed their failure to the lack of resources, or that their company is apparently not big enough to accommodate an IS security departments and maintenance routine costs.

In addition to these reasons, majority of the businesses cannot answer fundamental IS security issue questions related to;

- Performance measurement (how well is the IS security enhancing business requirement?)
- Security control profiling (what IS security processes are important, and the critical success factors for control?)
- IS security awareness (what are the risks of not achieving the internal data security objectives?)
- Benchmarking (what do other businesses do, and how can their results be compared and measured?).

Table 20 in the next page provides answers to these questions and summarises the common reasons for the failure of the IIDTRC prevention practices cited in the literature. The challenges of tackling these reasons have been, in some cases, attributed to reason some IIDTRC prevention practices have failed. The failure of the IIDTRC prevention practices have left the business management with little or no better option than to resort to available coercive security strategies (software security). But with this option, yet another question is whether the choice would better off?

If yes, the unavoidable question still comes: why have these available software-based IIDTRC prevention frameworks failed to prevent IIDTRC? Next section provides an answer to this question by discussing the strength and weaknesses of the available identity theft prevention frameworks.

Why Prevention Practices Fail?	**Explanation of the Reasons for the Failure of Internal Identity Theft Prevention Practices**
The perception that adequate and advanced IS security tools are already in place.	Company managers sometimes believe that having security software and firewalls, and being Sarbenes-Oxley (SOX), PCI and ISO related compliant are enough. They fail to know that unless these controls and regulations are consistently checked, the effectiveness of their security might not be assured. Dean *et al.,* (2012) suggest that it took more than 5000 companies until 2008 to join the International Association of Data Privacy that has been founded since 2000. The PriceWaterCoopers' (PWC) (2014) indicated that 80 per cent of companies fail to evaluate their spending on IS security resources or review if they are properly implemented and regulated. PWC (2014) suggests that most companies only struggle to evaluate their data security tools and regulations at the aftermath of the IIDTRC incidents. This suggestion agrees with Bielski (2005) that a few companies make strategic investment for their IT security.
Fragmented roles between the IS security management team	Shah and Okeke (2011) noted that some businesses lacks integrated data security approaches between the external and internal security auditors. In some cases, there is segregation in the roles of the sourcing and outsourcing security companies between the business and law enforcement agencies. For an effective proactive measure in the fight against IIDTRC, they suggested the business IS management and security audit team have to work in unison and jettison the perception of role segregation.

Why Prevention Practices Fail?	***Explanation of the Reasons for the Failure of Internal Identity Theft Prevention Practices***
Management Negligence	The evolving IIDTRC threats that might demand new tools and procedures are often treated with laxity by business owners and their management. At times, some of the security tools and regulations are not applied effectively. In the PriceWaterCoopers' (PWC) (2014) Survey, 56 per cent of businesses did not carry out any security checks of their external providers; instead they only rely on contracts and contingency plans. IS security-resource implementations could only be effective if they are well reviewed, regulated and properly applied. Many companies have fallen into this bandwagon of aftermath effect. The PriceWaterCoopers' (PWC) (2014) survey tracking of the past 3 years shows the degrading capabilities of IS security management across business organisations. In 2011, only 41 per cent of approximately 10, 000 executives across business organisations in 138 countries acknowledged that they have data security compliance and identity management strategy compared to 48 per cent in 2009. While only 39 per cent of these executives acknowledged that they reviewed their data security policies and regulations annually in 2011, more than 52 per cent did in 2009.
The huge demand on companies to maintain the increasing PID/I used by the consumers via e-tailing and e-commerce.	An average business organisation today handles at least 5 million customer's PID/I which encourages decentralisation of the data storage. This practice leads to vulnerabilities related to file transfer protocols (FTP), network shares and e-mail; which in turn pose many challenges of large file management, FTP software process, audit trails and version control, etc. (Forrester and Seeburger, 2013).

Why Prevention Practices Fail?	***Explanation of the Reasons for the Failure of Internal Identity Theft Prevention Practices***
The cost of Information System/Technology (IS/T) security management.	The ACFE (2014) survey suggests that some of the companies apparently consider themselves too small to bear the cost of applying security auditing for IIDTRC prevention. The failure of the business executives to conduct a cost and benefit analysis of IS security investments often lead them to believe that security cost outweighs the benefit. The PriceWaterCoopers' (PWC) (2014) survey indicated that 12 per cent of senior management give less priority to the data compliance management.
The perception of low expectations from the IS security and compliance management by the business managers	Popa and Doinea (2007) noted that many businesses managers often do not trust the capabilities of their security audit and compliance management. In some cases companies perceive data security audit as a complex practice and got intimidated by the daunting and demanding tasks of data security management.

Table 20: Why IIDTRC Prevention Practices Fail?

2.6 Identity Theft-Related Crimes Prevention Frameworks

As already discussed in chapter one (***Section 1.4***), there are few frameworks identified in the literature that are designed to prevent internal identity theft related crimes (IIDTRC). This is because the few frameworks aimed to generate general identity theft prevention across institutions. To justify the need for providing an independent framework for prevention of IIDTRC, the existing frameworks need to be reviewed to identify their limitations and establish the gaps to be bridged by a new framework. There are several models that appear in the literature concerning prevention of identity theft related crimes. The prevention of IIDTRC relies both on the human aspects of security management and on the computer systems security (Cappelli *et al.,* 2006). This distinctive characteristic of IIDTRC prevention underpins the reasons for available frameworks that have been designed in with generic IIDTRC prevention to cover all the two aspects.

As defined by the Cambridge Advanced Learner's Dictionary, a framework is a system of rules, ideas, beliefs or a supporting structure around which something can be built that is used to plan or decide something. This definition lays the concept of the available frameworks. However, little or none of the existing frameworks focus on a specific nature of crime and business sector to adjust the prevention for the specific requirement. The examination of the available framework is intended to provide the understanding and background for designing and extending proposed Role-based framework. The literature shows that the majority of available identity theft related crimes frameworks are designed based on the concepts (e.g. devices structure, systems designs, technology architecture and nature of crimes) of their predecessors. These on concepts on which available framework are underpinned are justifiable by the researcher's intentions.

However, in this case, it is important look at the suggestions made by other researchers on the IIDTRC prevention. Burkhalter and Crittenden (2010) points that the understanding of available frameworks would enable the researcher to understand and identify the research gaps needed for the recommendation of IIDTRC prevention framework. The critical consideration of their applicability is highlighted to evaluate their strengths and weaknesses. Hence, the commonly cited frameworks as they appear in the literature are discussed below.

2.6.1 Generic Internal Identity Theft-Related Crimes Prevention Frameworks

Several studies (e.g. Kardell, 2007; ACFE, 2014) agree that a less attention has been given to the studies of internal identity theft related crimes (IIDTRC) prevention in the context of a particular business organisation like online retail. Yang and Wang (2011) agree that generic IIDTRC prevention frameworks might be complex to be adapted in some business sectors because of differences in business operations, processes, organisational culture and technology.

ACFE (2014) noted there is a need for more research to be conducted in a particular business sector with critical emphasis on the roles of managing these differences in prevention of IIDTRC. In his research paper, Adams (2008) also noted that though identity theft related crime are omnipresent, their study has to be constrained to the key policy makers in a particular business sector or location to provide an effective result.

Cappelli *et al*., (2006) agree that the need to align business requirements with roles of management is indispensable for prevention of IIDTRC. They opined that the effective synergy of efforts interplayed with IT executives, managers, technical employee, human resources, and security officers could be a practicable tool in the prevention of IIDTRC. The testimony of the US successful implementation of Department of Homeland Security and Cyber Security Project confirmed that the need for the deployment of the effective management roles in preventing identity theft-related crimes in business sectors. In their research project, Cappelli *et al*., (2006) and Moore *et al*., (2008) agree that since IIDTRC involve majorly human elements manipulating IS, it would take the comprehensive and strategic inputs of the human roles to counter the crimes. Savirimuthu and Savirimuthu (2007) suggest that a deeper understanding of roles implications of managing complex systems like customers' data management is an important prerequisite to applicable IIDTRC prevention frameworks. They further suggested that the integration of complementary management with IT security management would be suitable strategy for mitigation of IIDTRC since these crimes are not only technologically motivated but mostly socially. In line with Savirimuthu and Savirimuthu's suggestion, Wang, Yuan and Archer (2006) acknowledge that more research needs to be done in the development of a framework for prevention of IIDTRC from the perspective of roles of the management.

In addition, Lacey and Cuganesan (2005) suggested that the collaborative effort of 'human resource security' – IT management, complementary data security and crimes prevention team are often overlooked in formulation of IIDTRC prevention strategies in the existing frameworks. Shah and Okeke (2011) agrees with Lacey, and pointed out that available frameworks fail to prevent these crimes because the strategies do not incorporate the roles of the complementary management teams (auditing, outsourcing firms, credit monitoring firms, law enforcement agency, etc.). Other researchers (e.g. Jamieson *et al.,* 2009, Pawson and Tilley, 1995, Stake, 1967) agree with Lacey (2005) and Kardell (2007) and suggest that development of robust IIDTRC prevention frameworks should be done from the perspective of a particular business. The study of IIDTRC prevention in the selected cases in online retail (a unique and distinct system) would help to simplify and understand the complexity of these crimes, and provides the background for effective implementation of the framework.

Table 21 on page 70 and page 71 summarises the collated literature on identity theft prevention frameworks. This review suggests that a few attentions have given on the roles of management in the prevention of IIDTRC.

Authors	Research focus	Key concepts	Research contribution
Shah and Okeke (2012).	Examination of the roles of management in IIDTRC prevention and internal data security.	Role-based framework for analysing prevention of Internal Identity Theft Related Crimes: Case Study in UK Retail Industry.	A systematic and integrated approach where the key components of management work in unison is required to prevent IIDTRC and maximise internal data security.
Steinbart *et al.,* (2012).	Exploratory investigation of the relationship between internal audit and IS security.	An exploratory model of the factors that influence the nature of relationship between ISA and IS security functions	The proficiency of the IS security auditors affects the quality of the ISA practices and could contribute to prevention of internal information theft.
Shah and Okeke (2011)	Exploration of existing literature on the propagation of IIDTRC, and the conceptualisation of these crimes in the retail industry.	The synthesis of Role-based framework for prevention of IIDTRC in retail industry.	IIDTRC prevention strategy should incorporate a collaboration of external and internal crime prevention actors, and all levels of an organisation should be given clear and specific responsibilities regarding internal data security.
Shararíri and Lababidi (2011)	Examination of the factors affecting internal auditors in the protection of computerised accounting IS from electronic penetration in banking operation	Enhancement of the factors that would contribute to the effective utilisation of ISA in protecting computerised accounting IS.	IS auditors should be fully aware of the operations of the business organisations, the activities of the e-fraud prevention team to be able to proffer IS security against internal data breaches and attacks
Moorthy *et al.,* (2011).	Evaluation of the impact of the role of IT on ISA in business organisation	Impact of the information technology on internal data security auditing.	Information Systems auditor has the responsibility of ensuring that the management and board of directors understand the liability of potential data security risks.
Schulze and Shah, (2009)	Investigation of communication strategies used by the e-commerce organisations (via websites) to battle identity theft related crimes.	Development of the Support – Trust – Empowerment – Prevention (STEP) Method for battling identity theft related crimes.	Few e-commerce organisations proactively prevent identity theft, provide supporting actions and inform consumers on how to protect their data against such crimes.

Authors	Research focus	Key concepts	Research contribution
Ji, Smith-Chao and Min (2008)	The examination of a theoretical view of identity theft crimes as the basis for business organisational information system designs (from system planner's perspective).	Systems Plan for Combating Identity Theft – A Theoretical Framework.	Various roles and the relationship of the identity chain should be coordinated in designing in a collaborated systems for combating identity theft crimes in business
Jamieson, Winchester, Stephens and Smith (2008)	The study of formation of identity fraud profiling definition, construction of a profiling classification; and identification of the barriers to the use of profiling by business organisations.	Development of a conceptual framework for identity fraud profiling and provision of frameworks main elements, their relationships.	Organisational identity fraud based profiling methodologies have information processing techniques applicable to developing fraud profiling models in the IS in business organisations; and that integration of these techniques reduce the incidents of identity crimes.
Vasiu (2004)	Examination of the risks of e-fraud in an integrated supply chain, and overview of significant adverse effect of e-fraud as a hindrance towards achievement of business organisational IS strategic objectives.	Development of a conceptual framework for E-fraud Control in Integrated Supply Chain of business organisations.	E-fraud prevention should be integrated to corporate board-level organisations' practices and business plans; and that management should be responsible for implementation and coordination of the human, technological, and financial resources necessary for controlling e-fraud in business organisations.
Wright (1998)	The exploration of the need for IS education among business organisations' employees	Development of framework for IS security training for employees.	To improve the IS security against IIDTRC, IS education must be integrated into the business organisations' practices and their data protection policies.

Table 21: Studies on Identity Theft Related Crimes Prevention

2.6.2 Software-based Identity Theft-Related Crimes Prevention Frameworks

British Retail Consortium (BRC) (2011) suggests that some of the existing internal identity theft related crimes (IIDTRC) prevention frameworks have focused on the implementation of software security. This suggestion is confirmed by some researchers (e.g. McCormick, 2008; Jabbour and Menasce, 2009) that focus on the software-based security related studies for the prevention of IIDTRC. While others (e.g. Bishop and Gates, 2008; Niekerk and Solms, 2010) focus on the combination of technology and process; while a few (e.g. Collins, 2003; Moore *et al.,* 2008) attempt to combine technology, process and people. The resulting frameworks from software-based studies are the scientific approaches that are only implementable in computer systems (Jamieson *et al.*, 2009). For instance, Le Lievre and Jamieson (2005) pre-conception Model of Identity Fraud Profiling was built based on the information processing which uses the trails from the computer systems to analyse the behaviour of the perpetrators. This frameworks application relies more on the use of computer systems than on the contribution of the IS management roles and end-users. This negligence of the contribution of these roles is one of the gaps in a body of literature this research tends to fill.

The review of the literature shows that many studies have neglected a crucial element of people: management roles. From the above table, software-based frameworks built with the concept of technology dominated the IIDTRC mitigation studies. 10 out of the 16 reviewed IIDTRC prevention model were based on technology. For instance, Nelliker (2010) and Park and Giordano (2006) applied the role-based access control techniques for analyses of the identity theft criminals' behaviours and profiles.

While Jabbour and Menasce (2009) presents Insider Threat Security Architecture (ITSA) framework to analyse the security scenario of the compromised IS by the privilege users, Ha *et al.,* (2007) applied the capability acquisition graph to demonstrate the criminal threats. These techniques are only implementable on the computer systems. The two models that are based on the concepts of the process by Niekerk and Solms (2010) and Bishop and Gates (2008) present the conceptual model to facilitate the argumentation of the organisational culture in information security systems.Only the system dynamics model and MERIT model by Moore *et al.,* (2008) and Greitzer *et al*., (2008), Cappelli *et al.,* (2006) with Keeney *et al.*, (2005) integrated these key elements: people, process and technology to proffer IIDTRC prevention framework.

While these contributions to IS systems security practices are theoretically possible to reduce internal data security vulnerabilities and IIDTRC incidents, researchers (e.g. Hofmeyr, and Forrest and Somayaji, 1998; Allen *et al*., 1999) suggest that it is practically infeasible unless the roles of human are central to the IIDTRC prevention strategies and practices. Table 22 summaries the review of some studies on IIDTRC prevention frameworks underpinned with technology, process and people.

Prevention Concepts	Researchers	Focus of the Model	No of Studies
Process	Niekerk and Solms (2010)	Conceptual model	2
	Bishop and Gates (2008)	Analyses of the IIDTRC threats	
Technology	Nellikar S (2010)	Scalable Simulation Framework	10
	Jabbour and Menasce (2009)	Insider Threat Security Architecture	
	McCormick (2008)	EDLP Programme	
	Ha et al. (2007)	ICMAP	
	Park and Giordan (2006)	Role-based Access Control	
	Butts (2006)	SPM-IT / MAMIT approach	
	Chinchani and Iyer and Ngo and Upadhyaya (2005)	End user security behaviours	
	Symonenko *et al*., (2004)	Natural Language Processing Systems (NLPS)	
	Schultz (2002)	6 indicator framework	
	Anderson (2000)	8 general approaches	
People, Process and Technology	Moore *et al*., (2008); Band *et al*., (2006)	System dynamics	4
	Greitzer *et al*., (2008); Cappelli *et al*., (2006); Keeney *et al*., (2005)	MERIT	

Table 22: Studies of IIDTRC prevention based on technology, process and people

2.6.3 Lessons from the Reviewed IIDTRC Prevention Frameworks

This chapter has explored within the scope of this research the available IIDTRC prevention frameworks and their contextual implementation issues. Researchers (Shah and Okeke, 2011; Prosch, 2009; Swartz, 2008) have attributed the failure for these frameworks' unsuccessful implementation to the issues of lack of clear roles and responsibilities given to the security managers and administrators, which in turn might lead to the following issues;

- Poor understanding of the nature of IIDTRC by IS security management (Newman and McNally, 2005; Schreft, 2007);
- Lack of effective internal investigation on methods used by the perpetrators of IIDTRC (Calvasina, Calvasina and Calvasina, 2006);
- Absence of comprehensive frameworks, strategy and data security tools (Jakobsson and Myers, 2007; Abagnale, 2007); if exist, these frameworks for prevention IIDTRC were developed in the context of generic business organisation which might be inapplicable to particular business like retail industry (CIFAS[9], 2010; BRC, 2011);
- Over-dependence on software security which may lead to inadequate and incapable monitoring of privileged users on information systems (Mills, 2007; Acoca, 2008).
- Lack of understanding of the role of people in integrating people, process and technology (Moore *et al*., 2008, Keeney *et al*., 2005; Cappelli *et al*., 2006).

These issues provide background to provide a comprehensive IIDTRC prevention framework that would tackle these issues. In addition, the issues provide insight on the imperative for evaluative research to assess how these requirements are met for successful implementation of any proposed framework for prevention of IIDTRC in online retail companies. Ekblom and Pease (1995) suggest that an applicability of any crime prevention framework would be limited if it is designed with the concepts of a technological-oriented approach of preventing crimes (that neglect the holistic approach that encompasses the human behaviour).

[9] Credit Industry Fraud Avoidance System is the UK Fraud Prevention Service which operates two databases: National Fraud Database (NFD) and Staff Fraud Database (SFD)

Ha *et al.,* (2007) agree with Ekblom and Tilley (2000) and argues that software technologies can foil data breaches, but cannot match analytic capabilities and creativity of human behaviour which is paramount in data security strategies, particularly in IIDTRC prevention. Hence, the next section discusses the theories in the literature that provide understanding of human behaviour.

2.7 Identity Theft Related Crimes Prevention Theories

Many criminology theorists (e.g. Quinney, 1970; Clarke, 1980; Ekblom, 1992; Cornish, 1994; Aker, 2000; Walker, 2006; Kramer, 2009; Wright, 2010) have studied crime prevention in various fields of human endeavour. As identity theft related crimes is one of the most prevent criminal activities, many theories (e.g. situational prevention, deterrence, rational) have focused on how they proffer prevention on identity theft related crimes by understanding why people commit crimes. The next section discusses situational crime prevention and deterrence theories in the context of internal identity theft related crimes prevention (IIDTRC). These theories are selected because of the attention they have attracted in the recent years in academic and security studies.

2.7.1 Clarke's 25 Techniques of Situational Crime Prevention

Clarke (1980) argues that there is a need to address the factors that creates crimes 'hotspot' (a location with high risks of crimes) and the characteristics that make people more vulnerable to victimisation than other. In other words, Clarke (1980) suggests that crime prevention measures need to concentrate on preventing crime from occurring and victimisation. These arguments form the basis for the concept of situational crime measures that constitutes the 25 techniques of the Clarke's Techniques of Situational Crime Prevention. The 25 techniques are built upon the five main measures:

- Increase the effort.
- Increase the risks.
- Reduce the rewards.
- Reduce provocations.
- Remove the excuse.

The five key measures that form the basis for the Clarke's 25 Techniques of Situational Crime Prevention is summarised in the table 23 below;

Increase the effort	***Increase the risks***	***Reduce the rewards***	***Reduce provocations***	***Remove the excuses***
1. ***Harden Targets:*** Anti-robbery system; quality locks	***6. Extend Guardianship***: Neighbourhood watch	***11. Conceal Targets:*** Do not keep valuables off sight office environment	***16. Reduce frustration and stress:*** Efficient queuing***;*** soothing lighting	***21. Set Rules:*** Agreements ***R***egistration
2.Control access to facilities :secure entries	***7. Assist natural surveillance:*** street lighting***:*** police hotlines	***12. Remove Targets:*** Removable car radios; Pre-paid phone cards	***17. Avoid Disputes*** Reduce crowding in pubs	***22. Post Instructions*** 'No parking' 'Private property'
3. Screen Exits Tickets needed, electronic tags for floor stock	***8. Reduce Anonymity*** Taxi driver IDs' How's my driving signs	***13. Identify Property*** Property marking Vehicle licensing	***18. Reduce Emotional Arousal*** Control violent pornography Prohibit paedophiles working with children	***23. Alert Conscience*** Roadside speed display signs' Shoplifting is stealing'
4.Deflect Offenders Street closures in red light district Separate toilets for women	9. ***Utilise Place Managers*** Train employees to prevent crime Support whistle blowers	***14. Disrupt Markets*** Checks on pawn brokers Licensed street vendors	***19. Neutralise Peer Pressure:*** Campaigns depicting what friends think of risk-taking behaviour (e.g. speeding and drug campaigns) "It's ok to say no"	***24. Assist Compliance*** Litter bins Public lavatories
5. Control Tools/ Weapons: Tougher beer glasses***;*** Photos on credit cards	***10. Strengthen Formal Surveillance*** Speed cameras Security guards	***15. Deny benefits:*** Ink merchandise tags**,** Graffiti cleaning	**20. Discourage Imitation:** Rapid vandalism repair	***25. Control Drugs/Alcohol*** Breathalysers in pubs, Alcohol-free events

Table 23: Techniques of Situational Crime Prevention (Source: Clarke, 1980)

Situational crime prevention is underpinned by several theories including, Environmental Criminology, Rational Choice and Routine Activity. The application of these theories and their contribution in the prevention of crimes can be extended to the prevention of internal identity theft-related crimes (IIDTRC) in online retail companies. This can be done by adapting the twenty-five Techniques of Situational Crime Prevention by the Clarke (1980).

The summary of how other measures of the situational crime prevention can be extended to the context of prevention of IIDTRC in online retail companies is provided in table 24 below. In addition, the instances in the literature where the use of the situational crime prevention measures has been applied are discussed.

Target-hardening: This measure can be an effective way of reducing IIDTRC perpetrators opportunities by obstructing the access of the employees through installing anti-copying computer screens applications in the call centres, and tamper-proof lockers for servers and routers.

Ekblom (1992) suggests that target-hardening approach which was used in the strategy of the anti-bandit screens on post office counters in London in the 1980s have cut robberies by more than 40 per cent. Clarke (1999) agrees with Ekblom (1992) and suggests that target hardening was also used in the ticket machines of the London Underground which has a significant impact in the reduction of losses of ticket sales.

Access control*:* Clarke (1999) suggests that this measure exclude potential offenders from places such as apartments, departments, stores and offices. Cornish and Clarke, (1989) suggests that the use of access control in a South London public housing estate and entry phones have a significant impact in reducing vandalism and theft. In the context of online retail companies, the use of effective personal identification numbers can be implemented to gain access to computer systems, servers, and customers shopping accounts.

Entry/Exit Screening: This is similar to access control but for the purpose to increase the likelihood for potential criminals to be caught if they fail to meet exit/entry requirements. Cornish and Clarke, (1989) suggest that this measure has reduced the books theft in the University of Wisconsin library by 80 per cent. In the context of prevention of IIDTRC, the use of fob has been introduced in many retail shops and call centres to regulate and monitor the staff movements.

Increase the Effort	***Increase the Risks***	***Reduce the Rewards***	***Reduce Provocation***	***Remove Excuses***
1. Target hardening: Physical locks for PCs, Anti-copying computer screens in the call centres; Tamper-proof lockers for servers and routers	***6. Extend guardianship watch*** Staff watching of visitors; Leave signs of occupancy, Disallow exchange of access privileges	***11. Conceal targets;*** Gender-neutral phone directories***;*** Minimise ID access of offices where sensitive information are kept.	***16. Reduce frustrations and stress:*** Efficient queues and polite service	***21. Set rules:*** Harassment codes***;*** Information security policies
2. Control access to facilities: Entry phones; Swipe cards for office access	***7. Assist natural surveillance:*** Improved office lighting; Open plan offices	***12. Remove targets:*** Removable data storages***;*** Clear desk and computer screen	***17. Avoid Over rowed office space:*** Reduce crowding in a call centres	***22. Post instructions:*** No pen, paper and pencil.
3. Screen exits: Reception desks	***8. Reduce anonymity:*** ID tags for staff	***13. Identify property:*** Property marking of PCs, Laptops and Sever Systems	***18. Reduce emotional arousal:*** Restrict access to how much money available in customers account	***23. Alert conscience:*** Create staff awareness to secure computers.
4. Deflect offenders: Server and Routers Rooms closures; Segregation of duties	***9. Utilise place managers:*** Two clerks for convenience Stores; Management supervision	***14. Disrupt markets:*** Monitor pawn shops	***19. Neutralise peer pressure:*** Disperse troublemakers at school	***24. Assist compliance:*** Regulated office checkout and regular holiday for staff; IT Security education for staff
5. Control tools/weapons: Disabling stolen cell Phones; Deletion of access rights for ex-employees	***10. Strengthen Formal* surveillance:** Security guards**;** Intrusion detection systems	***15. Deny benefits:*** Ink merchandise tags***;*** Encryption	***20. Discourage imitation:*** Censor details of modus Operandi; Prompt software patching	***25. Control drugs and Alcohol:*** Alcohol-free events – end of year parties and get-togethers.

Table 24: Adaptation of Situational Crime Prevention Approach for IIDTRC

These measures could be adapted by online retail companies as summarised in table 24 above to fit into the context of reducing the risks of IIDTRC. However, several researchers (e.g. Lewis and Sullivan, 1979; Clarke, 1999; Parker, 1998; Willison, 2006) have criticised the extension of the used of situational prevention. Clarke (1999) suggests that the measures may not be one hundred per cent effective due to the some issues such as:

- Technical or administrative ineptitude (Clarke, 1999)
- Measures being defeated by offenders or careless of victims (Cornish and Clarke, 2003)
- Too much vigilance reduces security consciousness (Clarke and Harris, 1992b)
- Measures may provoke offenders to unacceptable escalation (Hunter and Ray, 1997)
- Some measures facilitate rather than frustrate crimes (Ekblom,1992)
- Lack of proper analysis (user's needs) before introducing some measures (Clarke and Harris, 1992b).
- The detrimental effect of some measures on the environment (Akers, 1990; Willison and Backhouse, 2006).

Collectively, these issues summarised above suggest reasons for some situational crime prevention measures like generic and software-based framework (*discussed in the section in 2.6. 1 and 2.6.2*) may not work in intended ways. This is because measures what works in one setting may not do so in other settings due to organisational and management issues. Clarke (1999) suggest the need to be aware of these challenges and know which measures work best, in which combination, deployed against what kinds of crimes and under what conditions. He specifically noted that financial costs of particular crime prevention need to be assessed by businesses through developing a permanent in-house capability of their organisations. Hence, there is a need to explore more on other aspects of crime preventions that may contribute to the holistic view approach of internal identity theft related crimes in online retail companies. Next section discusses deterrence theory and its attributes in the IIDTRC prevention.

2.7.2 Deterrence Theory and its Attribute on IIDTRC

Quinney (1970) suggests that deterrence theory can be traced to the works of classical philosophers (e.g. Thomas Hobbes, Cesare and Beccaria, and Jeremy Bentham). These philosophers provide the foundation for modern deterrence theory in criminology that is classified into two: general and specific (Aker, 2000). General deterrence as the name posits is designed for prevention of crime in the general population, while specific is designed based on the nature of the proscribed sanctions to deter potential crime offenders from committing crimes in the future (Quinney, 1970). Typical instances where application the deterrence theory have been applied include the capital punishment – death penalty, and the used of corporal punishment – Shari'a/Islamic law in Nigeria which was introduced in 2001. The deterrence approach to crime prevention deters those who witness the infliction of pains upon the convicted fraudster from committing the crimes themselves (Morgan, 2010). Dobb and Webster (2003) and Wright (2010) argue that punishment as an element of a deterrence theory may be expected to affect conceptualisation of deterrence of criminals in two ways.

i. *Increasing the certainty of punishment*: This involves deterrent of potential offenders by the risk of apprehension. For instance, if there is an increase in the number of security guards monitoring online retail call centres, some employees may reduce their dishonest activities in order to avoid being caught.

ii. *The severity of punishment*: This may influence the potential criminal behaviour if he or she weighs that the consequences of their actions are too severe (Golden, 2002).

Wright (2010) suggests that these elements of punishment underpin the rationale behind 'truth in sentencing policies', to utilise severe sentences to deter some persons from indulging in criminal behaviour. Some critics (e.g. Willson and Herrnstein, 1985, Moyer, 2001) argue that it is difficult to prove the effectiveness of deterrence since only the offenders that have not been deterred come to the notice of law enforcement. Otherwise, the law enforcement may never know why others employees do not offend.

Wright (2010) argues that another reason for deterrence theory's limited application in prevention of crimes "*can be seen by considering the dynamics of the criminal justice system*" (Wright, 2010, p.3). If there is 100 per cent certainty of apprehending offender, there would be few potential offender.

For instance, as cited by the Wright (2010), since most crimes (identity theft related crimes as in this research) do not result in an arrest and conviction because of their complexity, the overall deterrent effect of the certainty of punishment might be substantially reduced. Other critics deterrence theory (e.g. Williams, Gibbs and Erickson, 1980; Sherdin, 1986; Hirsch *et al*., 1999; Tonry, 2008) agree that the absence of data on awareness of punishment risks makes it difficult to draw conclusions regarding the deterrent impact of the of deterrence theory. Hence, it may be difficult to measure the impact of severity of punishment as deterrence measure against identity theft related crimes on potential offenders who do not believe they will be apprehended for their dishonest actions.

However, Kramer (2009) argues that deterrence theory can be extended as a traditional security theory and superimpose on the prevention of identity theft-related crimes. Haley (2013) agrees with Kramer (2009) and argues that a strategic application of deterrence theory in businesses could reduce the costs of cases of internal identity theft related crimes. Goodman, (2010) argues that many studies on information systems security have not done more to apply tools of deterrence to the prevention of computer crimes. In particular, the deterrence theory argues to eliminate activities of the criminals by making costs and consequences to outweigh benefits that may be accrued from the criminal acts. Proponents (e.g. Gibbs, 1968; Quinney, 1970; Akers, 2000) of deterrence theory in the context of employee crimes believe that employees may choose to obey or violate the employee business policy after calculating the consequences and gains of their actions.

Instances in the literature have suggested the uses of legislation/law enforcement system and digital forensic investigation have proven to be great tools for deterrence of internal identity theft-related crimes in various business sectors.

2.7.2.1 Legislations/Law Enforcement: A Deterrence to the IIDTRC

While there is no silver bullet for effective prevention of internal identity theft related crimes (IIDTRC), the criminal justice system and law enforcement departments can make significant impacts on employees indulging in the crimes (Wright, 2010). Several researchers (e.g. Levin, 1971; Orsagh and Chen, 1988; Doob and Webster, 2003; Bavis and Parent, 2007) agree that criminal justice system increases in the *certainty* of punishment, as opposed to the *severity* of punishment, and it is more likely to produce deterrent benefits.

Many countries (e.g. UK, US, Austrian, Denmark, France, Germany) across the globe have continued to enact laws and legislations to match the advancement of the computer crimes from outside and within business sectors. The common legislations cited in the literature that have been enacted in different countries as discussed as follows;

Privacy Laws and Legislation: This has been used to protect the theft of personal identifiable information of individuals, especially customers of online retail companies. Since 1970, the US has used the Fair Credit and Reporting Act and Privacy Act to govern the processing, access, and disclosure of credit information. The same protection of individual privacy was aimed by the Canadian Privacy Act of 1975. The same data privacy protection and governance have been legislated across European countries – the Austrian Federal Data Protection Act of 1978, the Danish Acts on Private Registers, the French Act on Data Processing of 1978, the German Federal Data Protection Act of 1977 and the Swedish Data Act of 1973.Other Intellectual Property Laws have been cited in the literature (e.g. Organisation for Economic Cooperation and Development (OECD), 2013) which been introduced as a deterrence for the prevention of corporate identity-related crimes. These include;

- Intellectual Property and Copyright Law (e.g. Copyright Act of 1976): To deter the theft of trade names, ideas, secrets, computer programmes, personal knowledge, etc. that may be vulnerable to internal identity theft related crimes.

- Trade Secrets Law and Trademark Law: To deter the theft of ideas and trademarks of software and hardware of businesses and organisations.

- Patent Law: To deter theft software concepts and established products.

To ensure that the deterrence influence of legislation is extend to international regions where jurisdictions of privacy laws may differ from the originating venue, the Organisation for Economic Cooperation and Development (OECD) (2013) has introduced the OECD Trans-border Data Flow Guidelines to promote identity theft related crimes prevention. The guidelines are designed to prosecute and deter criminal for indulging in identity theft related crimes. For instance, in the US any employee that is convicted of trafficking or trading passwords or credit cards will be liable to Penalties of the Title 18, USC 1029 which is 15 years in prison for the first offence (Identity Theft and Assumption Deterrence Act 1998).

In the UK, violation of the Section 55 – unlawful obtaining of personal data, makes it an offence for perpetrators of internal identity theft related crimes and hackers outside the organisation to obtain unauthorised access to the personal data (Data Protection Act 1998, Section IV).

2.7.2.2 The Use of Digital Forensic as the IIDTRC Deterrence Measure

Several researchers (e.g. Farrington and Petrosino, 2000; Clarke, 1999) agree that an effective use of digital forensic as the internal identity theft related crimes (IIDTRC) has a deterrence effect on potential perpetrators. Clarke (1999) argues that increasing the perceived risks of committing crimes could deter the potential IIDTRC perpetrators. He further explained that this 'situational approach' of crimes prevention can deter an intended or potential IIDTRC criminal if the criminal knows that there is a certainty of being caught. Farrington and Petrosino (2000) agree with Clarke (1999) that digital forensic analysis play vital role for identity theft crimes under investigation, suggesting that fewer crimes would be committed in a business environment where there are such measures.

Other researchers (Sermon *et al.,* 2012; Walker, 2006; Rowlingson, 2005) have emphasised the importance of digital forensic as deterrence measure for IDTRC. Rowlingson (2005) suggests being digital forensic ready deters potential offenders because of the high risks that the criminal will be caught. If dishonest staffers know that the victim organisation is policing their corporate IS property with forensic technology, it rings the bell to the staffers that their organisation will 'always catch and prosecute thieves'. It may as well act as a psychological deterrent to potential computer related criminals (Walker, 2006; Gottfredson and Taylor, 1986).

Moreover, digital forensic investigation practice may encourage and intensify the mindset of natural surveillance to potential IIDTRC perpetrators (Sermon *et al.,* 2012). It provides demonstrative evidence during the courtroom prosecution of the suspect. Welch (1997) argues that evidence generated through digital forensic investigation convinces the jury beyond a reasonable doubt that the offender is guilty of the offence. Bhati (2010) study suggests that there is no doubt that digital forensic evidence immensely deters IIDTRC. In his study, '*Quantifying the Specific Deterrent Effects of DNA Databases',* Bhati (2010) tested the specific deterrent effect of digital forensic DNA evidence on crimes. He concluded that deterrence of digital evidence has probative effect ranges from 20 per cent to 30 per cent.

Bhati's (2010) finding agrees with the UK Home Office (2004) research that has similar deterrence effect of 20 per cent of the crimes committed. Taylor *et al.,* (2007) agree with Bhati (2010) in their arguments of impact of the deterrence theory and suggest that the knowledge of the fact that digital forensic evidence would be used in the IIDTRC investigation would deter potential offenders.

2.7.3 Lessons from the IIDTRC Prevention Theories

The evidence from the literature provides the understanding that the deterrent effect of criminal justice system and digital forensic investigation may substantially reduce the incidents of internal identity theft related crimes (IIDTRC). However, the impact of the deterrent on the prevention of IIDTRC might be dependent on the extent of awareness potential offenders have in relation to the deterrence measures. Though the critical impact of deterrence on prevention of IIDTRC could not be measure, deterrence has a significant impact on identity theft related crimes prevention. Based on the existing evidence in reviewed literature, there is a need to consider understanding of management roles in implementing the deterrence theories and the certainty that punishment would improve the likelihood that criminal behaviour would be detected.

2.8 Summary of the Literature Review

This chapter aimed to provide the understanding on: the Concepts of Internal Identity Theft Related Crimes (IIDTRC), Understanding of IIDTRC at the Workplace, the perpetration of IIDTRC, and IIDTRC prevention – practices, frameworks and theories. It has defined important terms that would contribute in understanding this current research and then reviewed IIDTRC in the context of the online retail sector. The last part of this chapter review existing practices, frameworks and theories in order to identify the properties that the extended framework in this study needs to include.

The key findings of the literature review are summarised as follows;

i. *Internal identity theft-related crimes (IIDTRC) ruin the reputation of the victims – companies and the consumers*: IIDTRC disrupt the operations of the online retail businesses and causes long-term problems (harassment from debt collectors, loan rejections, psychological and brands name damage) to the victims.

ii. *Few online retail companies endeavour to prevent IIDTRC*: There are instances in the literature that noted that ineffective prevention of IIDTRC is linked to issues which include insufficient clear policy that educates employees to be aware of the IIDTRC issues, neglect by management to ensure that their employees properly destroy unwanted information when deposing computers and papers. Many IS security managers are lax to update the online retail companies security technology tools such as servers, firewalls and antivirus.

iii. *Sparse studies on the prevention of IIDTRC, with a few studies on the IIDTRC prevention, are grounded with empirical studies*: The existing empirical studies present findings which are not applicable in IIDTRC prevention because of their poor research designs and generic nature of their IIDTRC prevention approach.

iv. *IIDTRC prevention face the following implementation challenges*: lack of effective internal investigation on methods used by the dishonest employees in stealing the identity information, inadequate monitoring of insider activities on the networks, insufficient control mechanisms for protecting paper documents, misappropriation of the information assets, inadequate protection of the personal information of the customers by the third parties service providers, and absence of comprehensive frameworks, strategy and data security tools.

Some studies focused more on the socio-economic impact of IIDTRC than on the prevention. Others focus on the scientific approaches that are implementable only on computer systems. Based on these findings, the researcher concludes and recommends that:

- a defined focus is required to identify a comprehensive strategy and data security tools for prevention of IIDTRC in online retail companies;
- the IS security management should be given a clear role and a well-define responsibility regarding internal data security;
- there is a need for internal collaboration of IS security management on prevention of IIDTRC.

- integration of both the external and internal environment for any adoption of IIDTRC preventive strategy, strengthening of strategic management and other forms of collaborations;

- adoption of strategies to consult, engage and communicate with stakeholders and employees in IIDTRC preventive frameworks; and

- ensuring proper education and awareness on the part of employees towards prevention of IIDTRC within online companies.

These recommendations form the basis of the role-based framework (RBF) for the prevention of IIDTRC. The recommendations re-enforce the need for the collaborative effort of IS security management in the prevention of IIDTRC. It can be drawn from the reviewed literature that the IIDTRC prevention may benefit from the suggestions/recommendations that aligning management roles would impact efficient and effective implementation of the IIDTRC prevention. These suggestions emphasise the need for the business management in the specific business context to integrate their overall management roles, processes and technology.

In addition, the suggestions in the reviewed literature provide the background on how this research would bridge these gaps in a body of literature. Thus, an effective IIDTRC prevention framework should have both theoretical and empirical underpinnings from the perspectives of the organisations and management under study. To bridge these research gaps, the concept of a role-based framework is discussed in the next chapter to addresses the arguments surrounding RBF concept – the theoretical and empirical grounding.

CHAPTER 3

THEORETICAL FRAMEWORK

3.1 Introduction to the Concept of Role-Based Framework

Role-based framework (RBF) is designed based on the idea that the effectiveness of a framework for prevention of internal identity theft-related crimes (IIDTRC) in a business organisation is dependent on the clarity of the shared roles of management. Therefore, effectiveness is dependent on clarity of integrated roles the management uphold (Shah and Okeke, 2011; Biegelman, 2009; Zhu, 2006). It focuses on the analyses of management on sharing roles and responsibilities in organisational setting where both the situational-based and offender-based IIDTRC prevention prevails (Ekblom and Pease, 1995). Thus, RBF assumes a basis of a paradigm that devolves the collaboration of shared roles to management involve in the prevention of IIDTRC.

The analysis of role-based framework is guided by organisational role theory (ORT). Chen (1990) suggests that building an empirically grounded theory as it is in this study requires a reciprocal relationship between theory and empirical data. He argues that understanding the theory underpinning particular crime prevention is essential for identifying the important attributes that ought to be used in an evaluation of the intended framework, as well as in articulating the assumed causal mechanisms for the development of appropriated outcome measurement (Chen, 1990). The RBF as a conceptual framework is proposed by synthesis of IIDTRC prevention practices and then used organisational role theory (ORT) as a theoretical lens to guide the study.

The analysis of the framework focuses on knowledge of recommended IIDTRC prevention practices, frameworks and theories reviewed in chapter 2 – 2.5, 2.6 and 2.7. The use of ORT in the examination of the concept of RBF guides the theoretical assumptions on which arguments of the study begins to emerge: can the effective sharing of management roles in relation to the IIDTRC practices be a likely key element of an IIDTRC prevention framework in retail industry? This question draws out the inherent arguments on how strategically can management worked in practices of preventing IIDTRC, whether their interactive management roles in the prevention of the crimes are characterised by conflict or consensus. Ekblom (2010) suggests that though know-how-knowledge of the process of the crime prevention plays a central role in the implementation of framework for any sort of crimes, the success depends on understanding the organisational management of the business under study.

Lawrence, Suddaby and Leca (2009) agree that the analysis of interaction between the crime prevention management and their immediate environment starts with understanding both entities as organisational configuration in the same socioeconomic setting with utmost aim of greater efficiency and productivity.

Hodgson (2006) agrees with Lawrence, Suddaby and Leca (2009) and suggests that it is not possible to carry out any theoretical analysis of how management in an organisation works without having adequate conception of what it is, and how it interrelates with its business environment. Hence, this study adopts organisational role theory (ORT) to explore these relationships, since roles in the context of hierarchical management system like retail business organisation are not defined in isolation but in a 'social or organisational net of role relationships' (Elliot, 1976; Cabri *et al*., 2006). Hence, ORT is premised on the notion that the manner in which management enact the arrays of roles (shared roles) in the task oriented hierarchical systems (retail industry) focuses on effective functioning of the roles within the organisation, and the interaction between roles and the impact this has on achieving organisational goals (Katz and Kahn, 1966; Biddle, 1986; Madsen, 2002).

3.1.1 Organisational Role Theory

The concept of organisational role theory (ORT) is one of the five major models of role theory developed by Biddle (1986) to examine role development in organisations. The concept of ORT describes and provides insight into the purposive actions of individual employees, management and organisations, as they relate to the field in which they operate (Kahn and Katz, 1978; Biddle and Thomas, 1979a; Lawrence, Suddaby and Leca, 2009). ORT concept has been applied by researchers in behavioural science, management, sociology, and psychology; for modelling authority, responsibility, functions, and interactions associated with management positions (Shah and Clarke, 2009; Zhang and Yin, 2006). In the study of how organisations can prevent crimes in their respective business domain, Ekblom (2010) and Sarnecki (2005) looked into the concepts of ORT and suggested that management in the organisations should in some way complement the shared roles and responsibilities; support each other in the environment where they operate. Ekblom (2010) argues that it might be helpful to conceptualise role-based crime prevention as an approach in order to provide integration of the software-based technology, process and people in IIDTRC prevention because it focuses the 'root causes' – lack of clarity of integrated IIDTRC prevention practices.

Biegelman (2009) agrees with Ekblom (2010) and suggests a need for interdependency of roles of the complementary management team for them to thrive in crime prevention in business organisations. Savirimuthu and Savirimuthu (2007) and Luhmann (2004) agree with these suggestions and argue that a deeper understanding of interdependency of management roles in business organisation is an important prerequisite for development of a strategic and coherent crime prevention framework.

The interdependency of management roles as articulated by Ekblom (2010), Biegelman (2009) and Sarnecki (2005), creates the basis for analysis of 'shared roles' among the crime prevention management in this study. The interaction of management becomes a role-based process where each party begins to share roles of each other, with clarity of valued interest of effective IIDTRC prevention (King, 2006). The interaction of various roles of human resources involve in crime prevention management underpins the analysis of the structure of the role-based framework. Based on the assumptions of the Ekblom (2010), Lawrence, Suddaby and Leca (2009), Zhang and Yin (2006), Sarnecki (2005), and Kahn and Katz (1978), an applications of the ORT in analysis of the roles of management can be derived. The ORT is thus applied in this study:-

- to help explain the crime prevention management roles and the implication of their relationship with other management (IT security, data compliance, law enforcement agencies, etc.) and how it can help to minimise employees indulgent in IIDTRC; and

- to help explain the impact of the clarity of crime prevention management roles/responsibilities and how it can help to maximise management performance in providing effective internal data security.

3.1.2 Understanding the Role of People in IIDTRC

Literature review in 2.5 of the Chapter 2 suggests there is research gap in a body of literature that internal identity theft related crimes (IIDTRC) prevention frameworks are not designed based on the people-oriented security, or rather integration of the both software security and human contribution. In addition, it was evidenced by the literature that the management of companies have depended solely on the implementation of software-based security in the prevention of IIDTRC that they neglect to consider integrating people, process, and technology.

The literature discussed above suggests that some of the IIDTRC prevention frameworks fail due to over-dependence of IS/T management on software-based security. This issue demands the need to provide IIDTRC prevention framework that encompasses integrating process and technology with people as the centre focus. In doing so, the discussion of the organisational role theory above has clarified that understanding the role of people can provide insights on the concept of RBF attributes of roles sharing. IS security management centred on people role in integrating process and technology is essential to achieve and maintain a secure IS in online retail. Software-based security grounded in technology, can be the most reliable in providing IS availability, confidentiality and integrity, but cannot be a substitute for people-oriented security. The need for people is indispensable, as IS owners, custodians, clients or users.

It has been understood from the outset of the review that it is the people aspect of IS security that gets online retail into the most trouble. Thus, there is need to equip the people by building their intelligence and decision-making capabilities to achieve the goal of IIDTRC prevention. Online retail companies can invest in the physical and technical measures such as authentication mechanisms, firewalls, and penetration and intrusion detection systems to defend external cyber-attacks. However, the insiders that have authorisation can bypass those measures to commit IIDTRC. The insiders are familiar with internal policies, process and procedures, which could be bypassed and exploited to carry out IIDTRC.

Anderson *et al.,* (2005) suggest that IIDTRC risk management should involve a comprehensive combination of behavioural, organisational and technical issues. Since internal identity theft related criminals utilise both technology and human techniques to perpetrate their threats, it is important to consider a combination of behavioural, organisational process and technical issues to prevent them. In the statement from Anderson *et al.,* (2005, p.8) that worked on Preliminary System Dynamics Maps of the Insider Cyber-threat Problem, they reaffirmed that;

> *"…because insiders are legitimate users of their organisation's networks and systems, a sophisticated technical capability is not necessarily required to carry out an insider attack. On the other hand, technically capable insiders are able, and have, carried out more sophisticated attacks, that can have more immediate, widespread impact, ….these technical insiders also sometimes have the capability to "cover their tracks" so that identification of the perpetrator is more difficult…"*

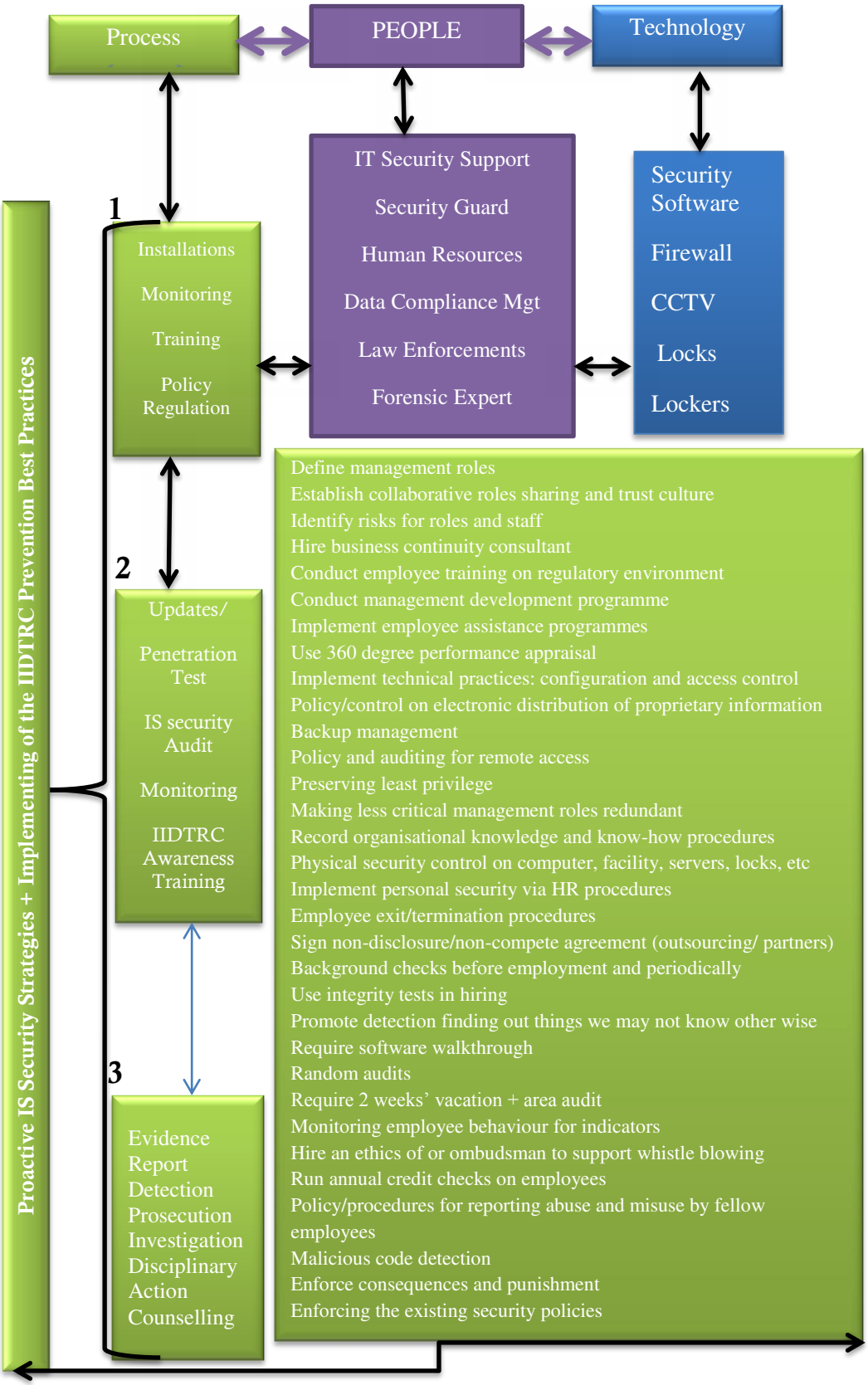


Figure 10: People as a Centre of Role-Based Framework Attributes

This statement suggests that it is important to understanding the people's role in the security of information systems in the online retail processes in order to mitigate IIDTRC risks – accidental or malicious. That is, it is important to understand the roles of the offender and users to regulate the way process and technology interacts. Since the IS security management is processed by the use of procedure driven by people, the major focus of IIDTRC prevention framework should be on people.

The procedure described in the ISO 9001:2000 is a way in which people – the IS security management, works to accomplish a task. The task here, as shown in figure 10, is the sequence of steps and actions required for prevention of IIDTRC in online retail. It is designed to function as a continuous process which shows how the IS security management can implement the recommended practices to reduce IIDTRC risks. The recommended practices are synthesised from the suggested IIDTRC prevention practices recommended in chapter 2. The practices synthesised in this section are not a comprehensive lists of all the applicable IIDTRC prevention practices. However, the practices are summarised to meet the scope of this research which is to provide IIDTRC prevention framework. This aim extends to clarify the task of IIDTRC prevention and identify how the roles of management can be aligned to meet the goal of preventing IIDTRC in online retail.

This task of getting people, process and technology to interact and cooperate is difficult to achieve (Hofmeyr and Forrest and Somayaji, 1998). This is why the human vector – the people has remained the weakest link in maintaining strategic IS/T security. This is the reason most IIDTRC *modus operandi* – social engineering, abetted collusion and collaboration build their attack strategies on human foibles. Human vector with the lack of awareness and desire for money or 'just wanting to help out' would always be a first target, or rather the criminal.

The figure 10 above is used to explain the direct and indirect relationship that should exist with each management role. Each of the separate boxes linked with thin arrows are indirectly related, which the thick arrows are directly related. These links depict the level of priority given to the labelled boxes: 'box 1' and 'box 2'; if those roles in relation to the responsibilities under the process, fails, and then 'box 3' would be required. For instance, the 'box 1' that is linked to 'people' (with thick arrow) comprises IT security, Data Compliance, Security Guards and HR. It contains IS security management roles that have possibility of sharing similar roles with each other.

3.1.2.1 Management Roles in the Prevention of IIDTRC

Several researchers (e.g. Kahn and Katz, 1977; Mitzberg, 1997) have used three specific categories of schemes to explain three categories of what management does: roles, functions and skills. Though, these categories are directly or indirectly related, this study focuses on the first: roles. Mitzberg (1997) refers to management roles as specific categories of managerial behaviour. Management roles are described based on different interrelated categories: decision-making, interpersonal relationship, transfer of information, reflection and taking actions.

The combination of these categories has a direct influence on the responsibility of IS security management in relation to the tasks of the IIDTRC prevention. In implementing the task of IIDTRC prevention, as noted above, it is important for every IS security management have a clear role for the management to collaborate (Oltsik, 2012). Collins (2003) and Udo (2001) agree that these roles are vital for a comprehensive IIDTRC prevention framework since the tasks and roles are the basic instruments for the security of the IS operations. So it is important that management roles interact and work together to support other cross-functional management.

The table 25 below summarises the descriptions of the key management roles common in online retail companies.

The interrelated steps shown in figure 5 above describe how the processes and technology centred on these management roles summarised in table 25. It provides holistic interaction of the concept that encompasses both the use of offender-oriented (people) and situational-oriented (technology) approaches in IIDTRC prevention. This concept would improve online retail IS security management posture. It provides capacity to control and monitor the technological aspects of security, as well as management adherence to established processes and procedures.

In addition, it enhances the IS security governance needs to leverage the human factors by regulating their interactions with technology. It would promote the intelligent workflows and process IS security management against potential IIDTRC risks. In addition, it is structured to provide the synopsis of the practical concept on which the structure of RBF attempts to depict.

Management Roles	***Description of the Roles in relation to Internal Identity Theft Prevention Practices***
Operational Management	Those that work in retail call centres and uses screening techniques to process customers' order for possible abnormality or mismatch of identity attributes – name, date of birth, account detail, etc. It requires the management to ensure that identity documents – customer and business, are cross-shredded before their disposal. For effective operation of this management, it is the role of HR to ensure that proper and essential training is provided (Hurst, 2010; Collins, 2003).
Technical management	These are the software engineers, web designers and data miners that use software security tools such as authentication kits, address verification system, digital signature, and encryption. This management depends on IS/T support to protect the IS security infrastructure from potential IIDTRC risks (Valrie and Rabih, 2013; Udo, 2001).
Managerial and Policy	This is role of the management that ensures the development of explicit policy regarding protection of security and privacy of business and customers. This involves implementation of policy strategy for safe preservation of business and consumers' data (Mills, 2007).This should emphasise the ethic of the company and reinforce on rewarding of employee. This would encourage and promote honesty in the workplace (Collins, 2001).
Risk Management	This role involves use of intelligent and strategic techniques to identify IIDTRC risks such as inconsistent in the transaction or customers order pattern. It also compares past and present history of consumer for inconsistencies, such as case of irregularity in use of credit card within short period of time (Duffin *et al*., 2006; Fichtman, 2001)
Resource and Control Management	This role demands the contribution of HR in counselling and training of employees. Since employees are the prime vector of IIDTRC, researcher (Collins, 2003; Newman and Clarke, 2004) have suggested that there should be effective employee control. In addition, this role manages vetting and screening of the employees.

Table 25: Key Management Roles in Online Retail

3.1.2.2 Role-based Framework: Relevance in Information Systems Security

Role-based framework (RBF) is designed to adapt, scale and provide necessary attributes – modules and tools. The attributes are modelled to build, orchestrate and plan IS security strategies, to integrate with cross-functional IS management and their tasks and workflows. It tends to streamline the IS security procedures by dynamically creating the necessary roles to eliminate potential management conflicts.

RBF is structured as a horizontal-wide model as opposed to the technical-vertical model. The structure is designed to enhance management workflows and IS security process platforms to improve agility, interoperability and vigilance (shown in table 26).

Key IS Security Attributes	***RBF Descriptions of IS Security Attributes in relation to Prevention of IIDTRC***
Agility	This is a key attribute of RBF. It tends to enable adaptive planning and delivery of IS/T security roles. This attribute would encourage evolutionary, flexible and rapid response to change in evolving IIDTRC trends in online retail. It would enable IS security management to prevent known IIDTRC risks. It would also provide foundation for effective responses to potential IIDTRC.
Vigilance	RBF is designed to provide management with the capability to integrate security intelligence to anticipate data security threats. It provides the attributes that would enable the management to evaluate risks and make informed decisions. It would enhance the adoption and collaboration of role sharing concepts in IS security management. This would enable the management to balance the technical controls with process for applying security to employees, partners and third parties that contributes to IIDTRC mitigation.
Interoperability	By adoption of integration of the people, process and technology (PPT) approach, IS security management becomes a single system with unified goal of IIDTRC prevention. The single system allows for easier monitoring and measurements. Importantly, it would enable the management to control that would minimise the impact of benign mistakes from employees' actions and processes related IIDTRC risks.

Table 26: Key IS Security Attributes and RBF Descriptions

3.2 Structure of Role-based Framework

Role-based framework (RBF) incorporates IIDTRC prevention practices recommended by IS security management from various business contexts. The IIDTRC prevention practices in this context is a set of documents, frameworks, ideas, information, languages, stories, styles and tools, that IS security management share. As defined by Wenger, McDermott and Snyder (2002), practice refers to the knowledge and the competencies of members, as well as to the specific things that they do. 'Members' refers to the IS security management. Surprisingly, there is little research on the 'actual practice' of identity theft prevention. The 'practice' of identity management is a contested terrain, unsettled in the minds of IS security management themselves, academics and policy makers (Wenger, 1998).

This section will, as far as is possible within the confines of this study, put together the 'best practices' of identity theft prevention in online retail. In so doing, this section draws conclusions on the recommended practices for preventing IIDTRC.

3.2.1 Role-based Framework Design Principles

Gercke *et al*., (2011) suggest that the cross-functional partnership that incorporates inter-dependent coordination of roles with skills sharing is one the most effective prevention practices in any areas of identity theft-related crimes. This suggestion could only be practicable in a defined business operation, online retail in this context, which may provide enable understanding of issues of internal identity theft related crimes (IIDTRC). Sharing of roles in relation to the prevention of IIDTRC is required in order to encourage leveraging, expanding of skills as appropriate, and support external relationship with agencies. Role sharing brings together expertise from diverse management backgrounds, HR, law enforcement, and IS security. Each management background holds information linked to IS security which, if shared, can provide comprehensive prevention views of criminal activity. This, in most cases, can be evidence-based practice. When these practices are based on equal sharing, equal level of power, mutual respect and understanding, then the IIDTRC prevention strategies would be implementable. The application and implementation of these practices have drawn from the suggestions of the researchers from these fields. This approach assumed that IIDTRC prevention should not be mere technological fixes but integrated IS/T security strategies – which explicitly or implicitly held by practitioners.

The purpose of the outlining common strategies of IIDTRC prevention found in the business organisation's literature is, primarily, to reduce the complexity in their analysis and application (as discussed in chapter 5 and chapter 6).

Although the IIDTRC prevention practices approaches have attempted to clarify their contextual analysis, as reviewed in 2.5; the use of concept of RBF has sought to provide clear role-based concepts over what could and should be implemented as IIDTRC prevention. This concept of RBF underpins the suggestions of scholars and more importantly of practitioners' need to increasingly work in IIDTRC prevention. Proponents of the intra-organisational management collaboration on which RBF analysis depends on, Ekblom (2010) and Sarnecki (2005), did not view their suggestions as being solely about improving the management roles interaction in their business environments in relation to crimes prevention. They believe that numerous conceptualisations of the crime prevention practices and theories delineate degree to which it might be applied to the management.

The research gap on the need for change in paradigm of IIDTRC prevention alluded to have been identified in the 2.6 chapter 2 – the shift from software-based and generic models of IIDTRC prevention to analysis of the integration of shared management roles, is attempted to be bridged with the concept of role-based framework .This analysis of the role integration approach is important in this context as it is through it that a new framework could be conceptualised. Because it is within the understanding of RBF attributes that IIDTRC prevention would be underpinned. Thus, understanding of the attributes of RBF and the diffusion of the responsibility for IIDTRC prevention beyond the either software-based or generic models is an explicit critic to the very idea of these concepts.

The 4 key attributes of the RBF are described in the table 27 below. These integrated attributes and elements are synthesised to ascertain this research aim and objectives. Collaboration of management in this context allows the IS security management team that implements IIDTRC prevention strategies to create structure that can help to effectively deliver organisations objectives which include and not limited to;

- IIDTRC prevention policy design and implementation,
- Encourage best practice to minimise IIDTRC risks,
- Maximise internal security performance, and
- Integrate management roles and responsibilities.

RBF Attributes	***Descriptions of Role-based Attributes in Prevention of IIDTRC***
Collaborative role-based monitoring	It would provide continuum and optimum roles/responsibilities across functional management team from foundation, proactive to preventive IIDTRC risks; **Foundation:** IS/T security warranty and remote support to law enforcements and outsourcing companies, and establishes their requirements with respect to service line agreements; **Preventive:** multi-management IS/T security support, clearly defined roles at the respective management level, dynamic and available management support.
Support capabilities	It tends to improve both the effectiveness and efficiency of IT/S maintenance and support. It provides opportunities for the Information security management systems (ISMS) to leverage on the competency and best results which may come from out-tasking the cross-functions to strengthen IS/T security strategy. It makes it possible for an informed, effective maintenance and technical expertise to be shared in a dynamic process.
Service-level agreements	RBF is customisable schema at hierarchical management levels to meet business information security management systems budgets, needs and strategies. This means that service-level agreements (SLAs) can now be linked dynamically to shifting roles, responsibilities and the workloads. Rather than being defined by static roles that does not reflect changing internal information security demand; the internal information theft prevention service level can fluctuate in response to IITRC risks; meets business' expectations for real-time role-oriented information security management; assures data security processes and business continuity through clear management roles.
Flexible support	It would help (information security management systems) ISMS to accomplish complex internal security tasks, manage or out-task IS/T security and IITRC. It provides flexible knowledge transfer to address range of IITRC prevention support complexities that might be beyond the expertise management support. It avails the option to choose management roles and services that better suits the business data security operation and structure; creates an information security optimised maintenance and dynamic IITRC prevention; minimises the ISMS service and roles that seem to clashes; provides integrated information security service management, optimisation, and flexible delivery choices and leverages on the expertise of cross functional management to reduce cost of IS platform as a service (PaaS) and infrastructure as a service (IaaS).

Table 27: Descriptions of the Role-Based Framework Attributes

Drawing from the analysis presented in the table 27 above, the concept of RBF is designed to draw from these attributes to conceptualise integrated management approach. It is proposed such that it would be grounded by the empirical study (via qualitative case study design discussed in subsequent sections). As a role clarification framework, RBF is designed to assist crime prevention management to improve their performance by assisting them to select and replicate practices appropriate to their needs and circumstances in the prevention of IIDTRC.

3.2.2 Role-based Framework: Sharing of Management Roles

RBF conceptualises IIDTRC prevention management as the body that encompasses complementary management team members – crime prevention, IT security, human resources and law enforcement agency. It classifies management roles in the form of a hierarchical level from the top management to the front line management. It follows the stages of crime prevention processes which include intervention, intelligence, implementation, collaboration and remediation measures. Intervention in this context refers to a combination of IIDTRC prevention strategies designed to change or improve the employees' behaviour or perception towards IIDTRC (Ekblom, 2010). The elements of intervention include but not limited to IIDTRC prevention awareness training, data protection training, IIDTRC incident reporting and whistle blowing. These elements can contribute immensely by promoting employees support, influencing the IS security knowledge and skills, and create a supportive working environment, policies and resources. Intelligence in this context refers to operations undertaken by IS security management to gather information that provide better understanding of the IIDTRC nature – cause and methods of propagation (Karn, 2013). Remediation measure in relation to IIDTRC prevention is the action that management takes to correct the damage done by IIDTRC perpetrators.

In this context, it is effective implementation and efficient collaboration by the management that can minimise the chance for the remediation process. While implementation is the translation of the chosen IS security strategy in action to achieve IIDTRC prevention goals and objectives, collaboration is the key that the management need to achieve this. The collaboration defines the IS security management working together towards a goal of mitigating IIDTRC (Gercke *et al*., 2011). It can be inter where the external agents (e.g. law enforcements, partners, outsourcing companies), or intra where the roles of manager are shared in the organisation.

These two last IIDTRC preventive processes (efficient collaboration and effective implementation of IS security strategies) forms the basic attributes of RBF. These attributes influences the impact of key components of the IIDTRC prevention strategies – policy, employees IIDTRC vigilance and awareness programmes, consumers' data protection, identity management, law enforcement, training, reporting procedures, and victims support. RBF is organised as a sequence of management level which emphasis the clarification of roles – IS/T security, IS audit, crime prevention, HR and law enforcement. The arrows, as shown in figure 11 below, depicts the interdependency of shared roles through monitoring, reporting, and collaboration between management levels

Based suggestion of IIDTRC preventions discussed in the chapter 2 above, an initial RBF for prevention of IIDTRC is proposed, which conceptualises the prevention of these crimes from a business organisation perspective; thus proposes following steps and measures. The measures identified in this context have their foundations in criminology (crime deterrence theory, Pearson theory and Cressey's fraud triangle theory), IS and management perspective (policy and risk management), and sociology (staff fraud, and white collar crimes, corporate frauds).

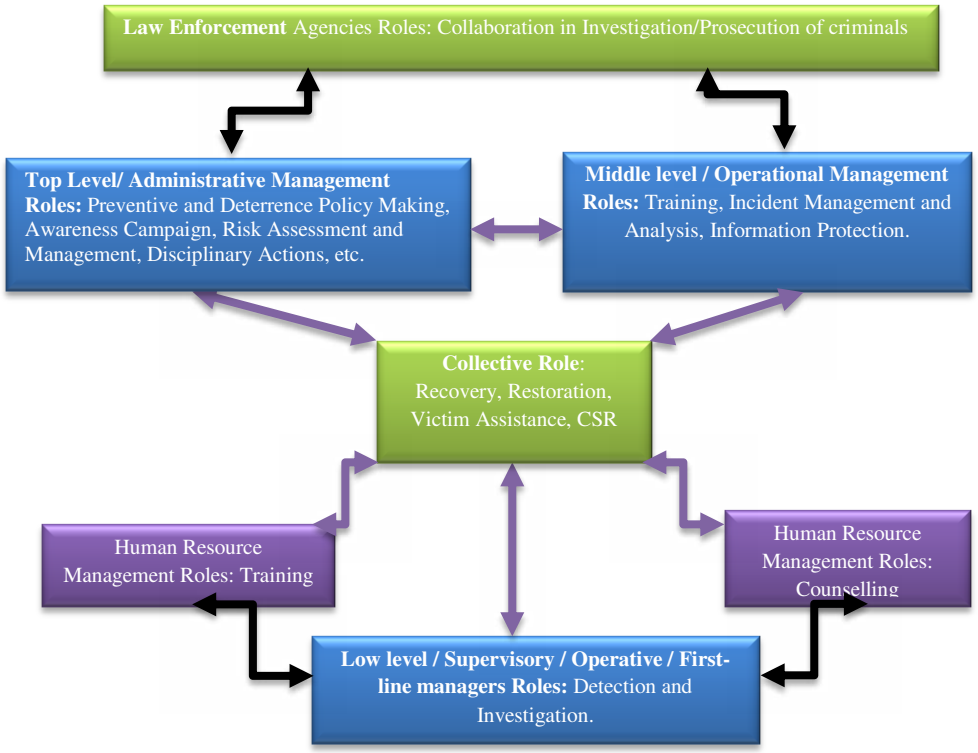


Figure 11: Role-based Framework

Management Roles

***Top Management*:** The role of the top level management for prevention of IIDTRC include: making of preventive and deterrent policies; risk assessment and management and disciplinary actions, etc. An effective internal identity theft policy within any business organisation is a necessary first step towards the development of an integrated strategy of identity theft prevention. The policy should also include other components such as definitive objectives, assumptions and directives which could increase the possibilities of discovery or decrease the probability of commission in internal identity theft related crimes in the organisation. There should be policy guides, clear procedures and internal rules for reporting and investigating cases of identity theft. Good policy statements are the basis for the scope of other steps to be built upon. Without prudent policy from the management of the organisation, other steps like risk assessment and management would not be effective. They should play hands-on role in ensuring information protection, detection of frauds, investigations and incident management so that prevention policies are taken seriously by all levels of an organisation. In doing so, their front-line experience would help them to develop more effective policies.

Middle-Management: The middle-level management in organisations comprises departmental heads and regional managers, etc. They are answerable to the top level management for functioning of their departments/teams while ensuring organising and directing roles which include: training, incident management and analysis and information protection. They implement the organisational goals, objectives and plans according to the directions/policies of the top management. They should be able to clarify and explain IIDTRC deterrent policies and guidelines from the top management to lower level management thus acting as a mediator between the two levels. The governing policies discussed above is supported by the technical policies, thus cover most rules and regulations in more details by adding to these rules that areas that relevant to the technology. These policies are meant for the technical custodians as they carry out routine security responsibility within the business.

The system and database administrators need to be kept abreast of the current technical policies within and outside the retail domain. As internal frauds threats are becoming more dynamic with fraudsters continuing to devise new techniques to exploit the easiest target, crime specialists suggested that retail industry should continue to invest in systems and controls to avoid being targeted as the weakest link (Financial Crime and Service Authority, 2009).

The advancement in the use of the information technology has enabled the criminals to continuing to refine and update their techniques. However, some of the new complex technologies that have been noted to have proven data and information security are biometric technologies, cryptography, authentication and certification and single-sign-on technologies. It has been proven that a right combination of these technologies built on well designed and enforced set of security rules and regulation always deter internal criminals from frauds (Schneier, 2004).

Nevertheless, the technical employees should know the technical guidelines and policies along with the effective application of the security software to increase their likelihood to prevent the cases of IIDTRC in online retail. Guidelines are procedural document lists and strategies adopted by business organisations. In most retail companies, the guidelines are developed based on the policy of the individual department. Employees pay lesser attention to these guidelines perhaps because of 'light-weight' of the consequences of their violations. There should be much attention given to the preventive guidelines to IIDTRC other the common data recovery plan guidelines, and the likes. The management at this level should be responsible for the coordination of different aspects such as the trainings of staff, incident management and rules enforcement policies and guideline.

The training of the employees in areas of information protection and data security should be their priority. They can organise seminars for the training of employees while ensuring effective incident management and analysis. This involves the management and analysis of the aftermath of identity fraud occurrences. The ability of the companies to implement rigorous incident management procedures relies heavily on the effectiveness of the middle management. Without such cooperation of the middle management and top management, IIDTRC would be difficult to manage.

Supervisory Management: - Also known as the first line management and usually comprises of store managers, shift supervisors, foreperson and the team leaders. Their basic role is the supervision of everyday business operations. Since first line managers have a strong influence on the employees and interact with them on a daily basis, they can play a vital role in the detection and investigation of identity theft related crimes. The major problem facing investigation of these crimes still boil down to lack of clarity of responsibility and less interaction or flow of communication between management and employees, thus making the cases of IIDTRC difficult to be proven when the perpetrators are caught. Supervisors can help address this problem by facilitating constant communication with the employees.

Roles of Human Resource Management: One of the most effective ways to mitigate the threat of IIDTRC such as collusion and coercion is to raise the awareness levels among all employees by the human resource managers. It is importance to let all the employees know the consequences of colluding or involving themselves in any form of internal identity related crimes. Organisations through human resources need to ensure that the members of staff are aware of whom to report the cases of fraudulent activities within the organisations. There should also be the provision for the employees to feel confident that the matter would be treated professionally. Base on this consideration that role of human resource management is very vital in prevention of IIDTRC; the structure of RBF depicts two loops on which the top and the middle-level management roles and responsibilities are hinged.

Roles of Law Enforcement Agencies: These are agencies that have a vital role to play in the IIDTRC as they mainly have the necessary power and skills to take IIDTRC cases beyond the reporting of incidents. Outsourcing the specialist teams to deal with these crimes is recommendable. They can also play a major role in educating businesses on the IIDTRC prevention measures. Assisting law enforcement and regulatory authorities in the fight against internal employees' frauds is vital for any business organisation, since taking legal action against the fraudster might be expensive and also an effective deterrent to others (ACAS, 2008). It is the roles of retail management to create awareness for the policies of data protection and the role of the law enforcement agencies to enforce the policies. The policy for prevention of internal identity theft-related crimes in retail industry encompasses many purposes:

- protection of stakeholders and information;
- set of rules for expected behaviour by employees, management, system administrators, security personnel, and users;
- authorise and define the consequences of violation of rules, authorise security personnel to investigate, monitor and probe;
- help to minimise security risks, define industry consensus stance on information and data security;

These policies and legislations discussed in chapter 2 above can be adapted in the context of online retail and created to be known across management, technical and employees' levels. In addition, other governing policy, technical policy and guidelines should be adapted to cover information and related identity proprietary data security. In doing so, the government data protection data and other important legislations are incorporated into the overall company's security policy.

Some of the online retail companies still neglect the integration of the government's data protection act such as Data Protection Act (1998), Freedom of Information 2000, and Computer Misuse Act 1990. Raising awareness among all employees about this relevant legislation relating to data security has been proven as one of the effective ways to mitigate the threat of the IIDTRC (Sommer, 2012).

Collective Roles: The employees and stakeholders in the online retail are expected to make more than just economic contributions. Both parties need to see and begin to recognise their responsibility to secure and promote information management in their companies (Listermann and Romesberg, 2009). This responsibility should not be limited to or beyond the level required by law, but extend to protection of identity proprietary information in order to achieve secure retail business operations. The application of concepts of Corporate Social Responsibility (CSR) in the context of prevention of internal identity theft in retail information systems security is, still, scare in both practice and theory. Although CSR have been applied extensively in many business sectors, it is still sparse in the context of retail information security management (Tsiakis, 2009).

Basel Committee on Banking Supervision encourages senior management to promote their organisation culture by exemplary life through integrity. There is the need for the online retail companies to stress the need for trust between the managers and employees. This would assist in monitoring employees' suspicious lifestyle that may pose potential detrimental effects to both the employee and employer.

Intelligence agencies and top human resource managers have listed various policies which could create a desired culture in every organisation. Some of these include: fraud management policy, employee fraud prevention policy, code of conduct or business ethics, disciplinary policy, fraud reporting policy whistle blowing policy, staff assistance policy and fraud specialist policy, etc.

Prevention of IIDTRC in online retail can also be provided through company CSR – a voluntary commitment to internalise in corporate pivotal decisions and strategy practices that contribute to social development. There is the need for the security managers to incorporate CSR activities in the corporate strategy of information security practices. Incorporation of motivational practices in the workplace by recognising/rewarding employees who promote honesty contributes to the development of ethical company cultures which in turn could reduce the cases of IIDTRC in online retail (Lewis, 2006).

3.3 Role-based Framework and its Propositions

Role-based framework (RBF) assumes that the integration of management roles sharing in a collaborative approach would be beneficial in implementing IIDTRC prevention practices. In practice, however, the literature review has shown that management role sharing is affected by number of attributes including people, operations, processes, organisational roles, and technology and management characteristics. These factors have been shown to be relevant to the success of information systems (IS) security in organisations. If an effectiveness of IS security is subject to the clarity of integrated shared roles the management uphold; then it is pertinent and important to argue that the applicability of RBF should be considered. As suggested by Chan (2002) that the ways of improving the application of information systems strategies can be found by asking three key questions:

i. What are key roles of integrated information systems that can clearly impact security management performance in the prevention of IIDTRC?

ii. What aspects of information systems security implementation are less likely understood in the prevention of IIDTRC?

iii. And what managerial practices improve the likelihood of information systems security integration in the prevention of IIDTRC?

Attempts to answer these questions would provide insights to the propositions on which RBF evaluation would be based: attributes those help or hinder integrated management in sharing roles and responsibilities in relation to IIDTRC prevention. Hence, the following propositions are deducted from the RBF:

P1: *Organisations with greater integration of the management are more likely to have effective collaboration between management roles (IS/T and crime prevention team) in prevention of IIDTRC (Zhu, 2006; Biegelman, 2009; Shah and Okeke, 2011);*

P2: *Organisations with greater collaboration of management roles are more likely to have effective implementation of IS security strategies required for the prevention of IIDTRC; Management with greater interaction implementing data security roles are likely to achieve organisational goal on IIDTRC prevention (Katz and Kahn, 1966; Elliot, 1976; Biddle, 1986; Madsen, 2002; Cabri et al., 2006);*

P3: *Management with shared understanding of data security operations are more likely to achieve better security strategy in preventing IIDTRC. Management role sharing is likely to affect the level of performance management in preventing IIDTRC.*

The clearly defined scope of the IIDTRC prevention practices is likely to result in more collaboration and improve performance by the IS security management roles. (Sarnecki, 2005; Hodgson, 2006; Lawrence, Suddaby and Leca, 2009; Ekblom, 2010);

P4: *The greater the inter-dependency of management in carrying out IIDTRC prevention roles, the greater the efficiency in IIDTRC prevention. A collaborative relationship between the management and employees is likely to improve the employees compliance with organisation's IS security policies. The collaborative relationship is likely to improve the effectives of internal data security by directing attention to the IIDTRC risks (Biegelman, 2009).*

As the RBF conceptualises these propositions, empirical research are needed to investigate which of these deductions are more perceived in the organisation. To provide these intended outcomes, the notion of the RBF evaluation is deemed imperative for the basis of its applicability in businesses. The evaluation would help to validate the propositions, which are summarised as follows:

- The collaboration of management roles has an impact on the implementation of tools required for the prevention of IIDTRC (Lawrence, Suddaby & Leca, 2009; Madsen, 2002); and

- Integration of the management has an impact on the realisation of the collaboration between management roles (IS/T and crime prevention team) in prevention of IIDTRC (Biegelman, 2009; Biddle, 1986; Katz and Kahn, 1966).

For instance, investigating the hands-on IIDTRC prevention awareness involving management has an impact on the prevention of IIDTRC. These proposition and potential results would direct the implementation of the RBF on how best to communicate, consult, support and engage employees, management and other stakeholders through the transition of the frameworks. In addition, the evaluation of the framework would identify:

- the steps of developing an effective performance management;

- the processes of assessing the key factors that may have an effective impact on the creation of secured information systems in business organisations with the collaboration of employees; and

- the training, technical know-how and skill sets required to implement and apply the guides and IS security practices.

3.4 Role-based Framework Evaluation: The Relevance in this research

Researchers (e.g. Newman and Clarke, 2003; Lacoste and Tremblay 2003; Newman and McNally, 2005) suggest that research should not only recommend practices for IIDTRC prevention, but should also evaluate the effectiveness of the strategies and practices. They suggested need to investigate how data security and crime prevention management adapt to IIDTRC prevention practices. They noted that the system of accessing, maintaining, and preserving information systems depends on the individuals who manage them for its security in the long run. Bressler (2009) and Bressler and Bressler (2007) also suggest that the models for the analyses of the complex inter-relationship between businesses and roles of management afforded to prevent the IIDTRC can be applicable through evaluative approaches. Ekblom (2010) and Sarnecki (2005) agree with Bressler (2009) and suggest the need to explore functional interaction between IS/T security management and crime prevention reference groups, and evaluate the extents of their roles in the crimes intervention and prevention implementation.

Newman and Clarke (2003) suggest that imbalance of the studies in a body of literature on crime prevention that has focused on theoretical recommendations of the crimes prevention policies should be corrected by investigating how to align the roles of management with relevant practices. Researchers (e.g. Anderson and Tresidder, 2008; Homel, 2010) suggested that evaluation of roles of management in implementing crime prevention strategies will help to identify and to prioritise the key concepts. Ekblom (2010) noted that evaluation of crime prevention framework enhances its applicability and plans to address resource constraints. English and Cummings and Straton (2002) suggest that an evaluation of the crime prevention framework can provide valuable information to enable security managers to plan improvements for future. Adhering to these suggestions, the key objectives of evaluations need to be identified for the Role-base framework. Thus, the next section overviews the concepts of RBF evaluation approach. It outlines various considerations made for the selected evaluation approaches.

3.5 Role-based Framework Evaluation Approach

The aim of evaluating the role-based framework (RBF), first, is to delineate, obtain and provide information which would be essential for describing and understanding RBF; and in making judgments and decisions related to its application. Secondly, to provide information on the functioning and outcome of RBF, the evaluation would provide description of the context in which the RBF would be operational, as well as the nature of its elements – human resource input, and the intervention processes to be used in its implementation. In the processes of the RBF evaluation through an empirical investigation discussed in chapter 4 and chapter 5, the underlying mechanisms or causal processes and outcomes of the framework would be achieved – that contributes to an understanding of the 'why' of the outcomes, as suggested by Pawson and Tilley (1995). For instance, empirical evaluation of RBF in the online retail company is done through case studies. It was done to investigate how RBF fits in the companies and to explore the challenges of managing IIDTRC prevention issues. The findings of the investigation form the basis for an analysis on how RBF attributes fits into online retail information security management. The findings guide the understanding of reasons for modification of RBF or what circumstances it might be expected to be applicable in other business settings.

Researchers (e.g. Mayne and Hudson, 1992; Obergfell-Fuchs and Kury, 2003) suggest two approaches commonly used in crime evaluation models: action-oriented evaluation and research-oriented evaluation. This research applied both approaches. The former leads to the priority given to information which is primarily useful for the RBF modification within a relatively short time frame and this is the rationale for the case studies discussed in chapter 4. Research-oriented evaluation, on the other hand, allows a high premium on the methodological rigour (Patton, 1990). Rather than being applicable for modifying crime prevention framework, Sherman (1997) suggests that research-oriented evaluation is suitable for longer-term application of the crimes prevention framework. And this is one of the rationales for further investigation of the application of the RBF attributes through participant observation case studies. This research, while applies action-oriented evaluation, incorporates other elements of crimes prevention model evaluation suggested by Owen and Rogers (1999): clarificative, impact, monitoring, interactive, and proactive. The element of a clarificative evaluation dictates the rationale of archival analysis which is introduced in chapter 4, discussed in chapter 5 and applied in chapter 6.

Archival analysis approach, as a clarificative tool for RBF evaluation, complements the review that has been used for the conceptualization of RBF. These research methods are adopted to clarify the underlying rationale and assumptions about how the components of RBF might be linked to produce the desired outcome.

In addition, the elements of an interactive, monitoring and proactive are applied in the action-oriented of all empirical investigations of case studies. These elements, in the respective cases, direct the evaluation of the actual need for the RBF framework. It directs the monitoring of its delivery for management decision making and accountability purposes. This element would guide the application of RBF. It would help to determine to what degree or extent the RBF objectives have been met based on the assessment of the intended/unintended outcomes, and to justify whether RBF should continue to be implemented in its context of its applications or in other settings, and if so, whether, modifications are required.

3.6 Summary of the Theoretical Framework

This chapter has synthesised lessons learnt from the literature review in Chapter 2 to conceptualise Role-based framework. It has used the organisation role theory to analyse;

- the concept of integrating both the external and internal environment for any adoption of internal identity theft preventive strategy;
- that creation of clear roles and shared responsibilities are necessary to prevent IIDTRC;
- the adoption of strategies to consult, engage and communicate with stakeholders – the cross-functional management and employees in IIDTRC.

Based on these concepts, the principles of identity theft-related crimes practices and role sharing has been extended to design the role-based framework which distinguishes this research from other studies that have provided the generic frameworks. Then the concepts were summarised in research propositions. This approach to the IIDTRC prevention framework aims to provide evidence-based results prevention of an IIDTRC incident. This chapter concludes with the summary of the rationale and research approaches for evaluation of the role-based framework. The discussion of the rationale and research approaches is provided in the next chapter.

CHAPTER 4

RESEARCH PHILOSOPHY AND METHODOLOGY

4.1 Introduction

In social sciences, business information systems, in particular, the choice of different research methodologies used by researchers always dictates the research paradigm (Hatt, 1985; Smith, 2000). Several researchers (e.g. Mitroff and Mason, 1973; Davis and Hamilton and Ives, 1980; Hirschheim and Klein and Lyytinen, 1996) argue that there is no clear suggestion for the best research methodology to be used in the study of Information Systems (IS) security. Various research methodologies differ in underlying paradigms and philosophies of which many may or may not be compatible (Lyytinen, 1987b; Smith, 1998). It is then left to the volition of the researcher to choose the research paradigm that provides the better analysis of the research problem under investigation (Smith, 1998). As defined by Kuhn (1970) in The Nature of Science Revolution, a paradigm is the underlying assumptions and intellectual structure upon which research and development in a field of inquiry are based.

By examining a variety of research philosophy available in the domain of Information Systems (IS) security, this section provides an analysis of the underlying assumptions and intellectual structures upon which this research is based. It attempts to answer the questions: which research paradigm builds the knowledge of IS security (Ramiller and Swanson, 1993)? In doing so, this chapter has two aims. First, it contributes to the understanding of the place of internal identity theft related crimes (IIDTRC) prevention in the philosophy of Information Systems security research. Secondly, it examines an appropriate research method for examining the roles of IS security management in relation to their practices in online retail companies.

4.1.1 The Philosophy of this Research

Selecting a suitable research methodology that best answers the research questions in this study was not methodologically led, it was based on the philosophical stance of this research background, the research problem and research questions. This section provides an answer to some of the epistemological question of this research problem by exploring the ontological view of this research. Having explored several research paradigms, constructivism and interpretivism are adopted based on the following rationales.

Constructivism: Since this study aims to explore the management roles that are based on the behaviour and interaction of individuals, the concept of constructivism is deemed appropriated by the researcher. Constructivism claims that truth is relative and it is dependent on one's perspective. It is dependent on the theory of knowledge which influences the interaction between the researcher and the participants throughout the research design (Little and Carter, 2007). Constructivism as a research paradigm recognises the importance of the meaning of subjective human creation (Charmaz, 2000). Searle (1979) suggests that constructivism is built on the concept of a social construction of reality which enables the participants to tell their stories and at the same time enhances the collaboration between the researcher and participants. As the case is in this research, it has set out to explore reality – what the nature of the IIDTRC is, by investigating roles of management in preventing IIDTRC. The subject 'nature of the IIDTRC' describes reality (research problems) and the researcher need to explore research problem to provide the better explanation of the reality (Lather, 1992).

Interpretivism: This paradigm allows close collaboration between the researcher and participants – information systems security management in the selected online retail companies. Huberman and Miles (1994) argues that research which involves collaboration between researcher and management, that focuses on an issue identified as significant by the participants and which is carried in the organisation is more likely to have impact on practice. Hence, there is a more pronounced impact of research findings on practice if the researcher-participant relationship involves interaction over a length of time (Crotty, 1998). And this is the case in this study where the researcher and participants interact before and during the data analysis and write-up phases.

Another reason for using an interpretivist concept was that it allows the researcher to acknowledge and explore the complexities of different organisational issues (in this case, online retail companies in relation to IIDTRC prevention).

In addition, interpretivist status enables the researcher to connect the findings and determine the context and then imagine whether the measurement procedures would yield the same data if replicated in the context of this research (Brooke, 2002). Throughout the three years of this research project data were gathered from a number of different online retail companies, each with the potential for differing IIDTRC prevention practices and management roles and where employers worked together and defined their relationships in a multiple of ways.

Constructivism/Interpretivism: In terms of this epistemological analysis, interpretivism is closely linked to constructivism. Thus, this close link underpins the rationale of the researcher to adopt the status of these paradigms in this research. Interpretivism asserts that social reality and laws of science (natural laws) are different and, therefore, require different kinds of methods (Fay, 1996). While the natural laws seek to clarify consistencies in the data to deduce laws (which is excluded from the scope of this research), the social reality deals with the actions of the individual which is contextualised of this research. The interest of this research focuses on exactly those aspects that are unique, individual and qualitative, which is relative and dependent on one's perspective. And this interest is exactly a major stance of constructivism. The researcher's status on the interpretivist and constructivist paradigm which encourages that there is no absolute reality; that truth is not singular; and knowledge is created by the knowers, and there are multiple realities and they are created by our lived experiences. This status geared the researcher's view on the attempt to generate 'unknown' realities through individual business operational experiences. And this is really important in this study; to be able to give voice to the participants and to also give the right to the researcher to interpret and to be able to tell a story about this research in the end. Since interpretivist stance is a major anti-positivist, it looks for '*culturally derived and historically situated interpretations of the social life-world'* (Crotty, 1998, p.67). The world (of information systems security issues in retail companies) can be interpreted through the classification schemas of the human mind (perceptions and experiences of research participants from retail companies) (Williams and May, 1996).

Phenomenology: Based on the aim of this research, a phenomenological concept of interpretivism was adopted to complement the constructivist/interpretivist status of the researcher. Phenomenology holds that attempt to understand social reality (research problem in this case) has to be grounded in participants' experiences of that research problem (Tesch, 1994). Hence, phenomenology requires that researcher and participants must lay aside their prevailing understanding of the phenomena (research problem in this case) and revisit the problem in order that new meanings may emerge (Remenyi and Williams, 1995). In other words, this is gaining the subjective experience of the research problem by the researcher through 'assuming' the place of the subject (Chen, Shek and Bu, 2011). Hence, phenomenology becomes an exploration, via prevailing cultural understanding and personal experience. In doing these, the research ascribed values not only to the subjects, but also to the interpretations of the research (Paul, 2004).

Since this logic of phenomenology seeks to find the internal logic of the subject which is far from using a theoretical model that impose an external logic, it supports the stance of this research which tends to extends the application of the Role-based framework.

Phenomenology/Ethnography: Though, Tesch (1994) and Carter and Little (2007) distinguish between phenomenological research and ethnography, the researcher adopted the epistemological stance of both approaches in this research. While phenomenological research and ethnography are based upon interpretation and description, ethnographic research is focused more on culture and phenomenology focuses on the human experience of the 'life-world' (Tesch, 1994). While the unit of analysis of ethnography is often 'sites', phenomenological researchers make use of 'individuals'. Phenomenology makes use of interviews, while ethnography' prime mode of data collection is observation – either as participant/outside observer, which is sometimes supplemented by interview data for clarification (Easterby-Smith *et al.,* 2002). These suggestions were applied in this research design. For instance, the first case study of *RetailGroup* involved semi-structured interview and the investigation of security audit practices were conducted in the 'sites' of the selected companies.

4.1.2 The Choice of the Research Methodology

To explore this research problem, a qualitative case study is adopted based on the philosophy of constructivism and interpretivism (Yin, 2003; Stake, 2000). Hence, the choice of the qualitative case study in this research was determined by the theoretical paradigm (Baroudi and Orlikowski, 1991; Layder 1993; Guba and Lincoln, 1994) and the circumstances of the reality to be researched (Glaser and Strauss, 1967; Eisenhardt, 1989; Yin, 1994). This research adopts qualitative case study to ensure methodological rigour due to the nature of research problem (Stake, 1994) – understanding human behaviour, and to contribute to the debate on the application of qualitative study in the IS security research. The choice of qualitative case study is also based on the research paradigm – *"basic set of beliefs that guides action* (Guba, 1990, p.17)", which is premised on the combine beliefs of ontology, epistemology and methodology. Since this research aims to develop of IIDTRC prevention framework, which constitutes management actions and roles – IS security rules and policies, the constituent elements of the qualitative case study: archival study, semi-structured interview and participant observation, are required to investigate the actions and roles.

These chosen research methods enabled the researcher to build, from ontological stance, how the research relates their existence or nature of social entities, their interaction and behaviour. Based on the concepts of ontology, the researcher sees the research problem from both constructivist and interpretivist point of views. The research problem is constructed based on perspective at a given place and time, and at the same time interpreted as a series of established elements whose behaviour and existence ultimately can be explained by underlying rules.

The motive of the researcher for using qualitative research builds on the suggestion by Myers (1997) that the ability of human beings to talk is what distinguishes them from the world around them. Denzin and Lincoln (2005) agree with Myers (1997) and suggest that qualitative research is an activity that locates the researchers in the world around them, of which they attempt to study things in the natural setting, make sense of, and interpret phenomena in terms of the meaning people bring to them. Smircich and Morgan (1980) add that qualitative research is an approach rather than a particular set of techniques and that its appropriateness is usually derived from the nature of the social phenomena to be explored. Thus, qualitative research is chosen to help the researcher understand the socio-cultural context (online retail companies) and the people (management) within which they operate. The researcher also buys in the suggestion of Algozzine and Hancock (2006) that qualitative research methodology 'is such', an intermediate research approach which allows the researcher to match philosophy, methodology, and the research problem.

Saunders *et al*., (2007) supported this point by expressing methodology as a theory and analysis of how research should start; it provides justification for the methods of a research project and not the project themselves. Saunders *et al*., (2007) emphasise more about the term 'theory' by referring methodology as the theory of how research should be undertaken. In agreements with the above notions, Bryman (2008), Hakim (1994) and Outhwaite (1983) concur that the theory of research methodology, at its best, is a catalyst for change, it is not an end itself; rather, its insight introduces a critical moment into status quo which optimally leads to the corrective changes of the repressive reifications in existing conditions. Hence, as noted earlier, the researcher believes that interpretive qualitative research grounded in constructivism would be 'a catalyst for change' in understanding the nature of IIDTRC preventions. It is an instrument that would be used to shed lights on the dark areas of IS security research as it relates to IIDTRC prevention.

Philosophical concept	Related research questions	Qualitative
Ontological	What is the nature of reality: what is the nature of IIDTRC in online retail?	Interpretivist: Reality is subjective and multiple as would be seen in this study (multiple case study with many participants)
Epistemological	What is the relationship of the researcher to the researched? Axiological: What is the role of values? Rhetorical: What is the language of research?	Researcher interacts with 'being researched' Axiological: Value laden and biased Rhetorical: Accepted qualitative words / Informal evolving decisions/personal voice
Methodological	What is the process of the research	Accurate via verification; Context bound; emerging design-categories identified during research; inductive process; pattern, theories developed for understanding

Table 28: Concept of Qualitative Research Paradigms

(Adapted from Creswell, 1994)

Based on the above arguments and suggestions summarised in table 28, the place of quantitative research methodology in this research was not considered. This is because of the 'strictly' positivist concept of the quantitative research which emphasises the measurement and analysis of causal relationship between variables; carried out in a 'value-free framework' (Denzin and Lincoln, 2005).

Besides, due to the concepts of quantitative research having been originated from natural sciences, it is deemed to be more relevance to defined relationship, numerical methods and surveys. And this is not the case in this research. Hence, the relevance of qualitative research in this study is considered.

4.2 The Relevance of Qualitative Research in this Research

The question this section answers is *what qualitative research method is relevant to this research?* The researcher views that the quantitative based positivistic concepts of 'value free' and 'one world' would not be helpful (Denzin and Lincoln, 2011). Thus, both the qualitative-based research approaches fit well with the scope and aim of this research. Since information systems management research is transdisciplinary, Gibbon *et al*., (1994) suggest, it is perhaps qualitative research methods that can largely accommodate the transdisciplinary nature of information systems management research for reliable research results. Madan and Starkey (2001) suggested that qualitative research methods encourage researcher and participants to engage passionately in research activities. It is in such research endeavour that the findings of the information systems management research would be relevance to business organisations.

4.2.1 The Relevance of Case Study in this Research

Case study research enables researchers to develop an inquiry that may lead to a more informed background for theory development (Yin, 1989; Eisenhardt, 1989). As noted by Glasser and Strauss (1967), a qualitative case study with qualitative research design is a suitable research instrument to provide an empirical data for theory building. It allows for analysis of the data from the participant's perspectives that contributes to building a grounded knowledge. Several researchers (Yin, 1989; Stake, 1995) suggest that a qualitative case study should be chosen in typical research context; first, when the research problem requires the researcher to seek the contextual meaning within a bounded and intricate system. And this study is the similar context since the researcher seeks to examine the nature of IIDTRC prevention in the online retail companies as a bounded organisation setting. It provides the researcher an advantage and a way to explore and understand the phenomenon and context when the boundaries between them are not clear (Yin, 1981).

As noted by Cooper and Emory (1991), case study establishes greater insight into boundaries and phenomenon under study. In this study, the focus is on the roles of the management in the prevention of IIDTRC. The emphasis is on studying IIDTRC issues from the boundary of the peculiar nature of the online retail management.

The use of case study would enable the researcher to deal with management intricacies, process and roles. It would also help the researcher to focus on the relationship between participants and the organisational setting (Foster, 1991). Second, Hirschman (1986) and Merriam (1988) suggest that qualitative case study research is suitable when the research activity is an inductive theory building. And this is similar to this research's case study design. The case study provided a greater analysis of the dynamics of management roles in the prevention of IIDTRC. It also helps the researcher to establish a rich understanding of the management situations as they relate to the data (inductive) that emerges from the research. The results of the analysis contribute to theory building based on *a prior* theory.

Figure 12 shows research activity of this study with emphasis on the relevance of *a prior* theory to the research design (Yin, 1993; Huberman and Miles, 1994). It starts with the initial identification of the research problem and the building of *a priori* theory via review of the literature. It continues with the collection and collation of the data. And finally to the analyses of the data that produces final theory development and generalisation (Coote, 1994).

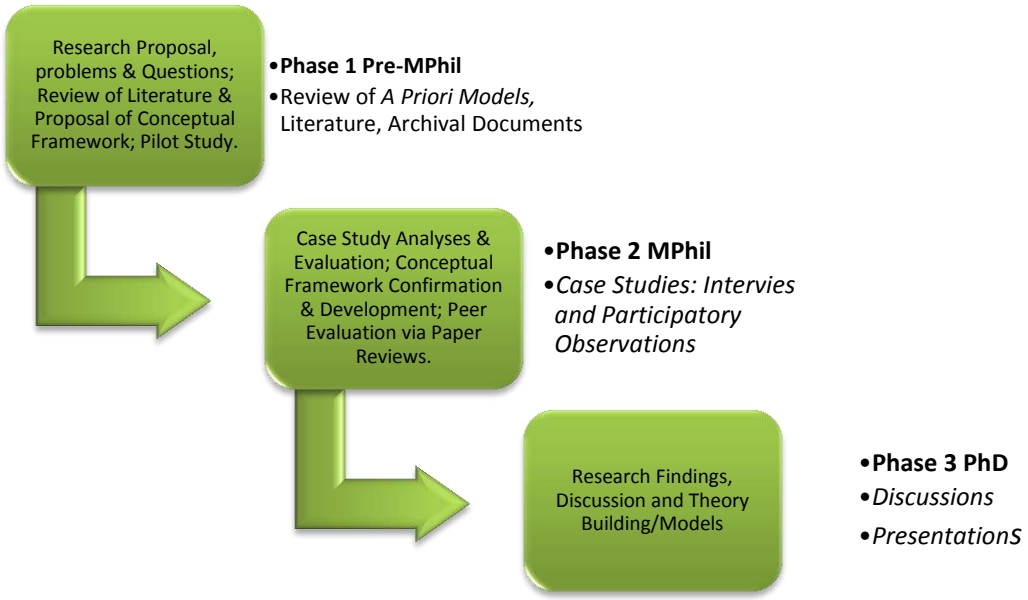


Figure 12: Research Development Stage

The third is when the research activities are focused on context that has specificity (Merriam 1988; Eisenhardt 1989). Also, the case of this research is a similar example as the nature and the prevention of IIDTRC are being studied in defined context of retail companies with IS security/crimes prevention managers as the target population.

In general several researchers (e.g. Yin, 1989; Hakim, 1994) suggest that the application of case study in research should be considered when: 'situation of theory development', 'research where boundary between phenomena and context are not clearly defined', qualitative and exploratory and explanatory', 'empirical enquiry', 'research where multiple sources of evidence are used', embedded case studies were sub-units of analysis.

For instance, a case study in IS security of disaster at a University by Ayyagari and Tyks (2012) sought to address the: cause of the disaster that leads to data breaches and security management functions in handling the security laxities. A case study was chosen because the case was security functioning of university management, but the case could not be considered without understanding the context of the management of the University; and more specifically, the IS management and management structure and setting. It was in these structures and settings that the functional roles were developed and utilised. It would have been impossible for the researchers to have had a true picture of the University's IS security breaches without considering the context within which the circumstances that led to the occurrence of the disaster.

Similarly, this research adopts the case study as well-defined research approaches to empirically provide answers to the research questions. The *a priori* theory analysis at the outset of this research provided a background to define the conceptual framework (as suggested by Guba and Lincoln, 1985). The *a priori* theory analysis refined the focus of the reviewed literature and helped the researcher to develop a suitable research design for the data collection (Yin, 1993).

Figure 12 above shows the developmental chart of this research design with case study design linking the initial and final stage. The arrows show phases from 1 to 3, as they were spread out from MPhil to the PhD.

The case study as suggested by (Eisenhardt, 1989), is used in this research to study the practices, roles and workings of management in the prevention of IIDTRC. Neuman (1994) and Yin (1994) suggest that case study design enables the researcher to recognise the prior theory that would be vital to the research design. It enables the researcher to carry out the study in a methodically sound way. Through the review of the literature, this research has identified and confirmed the statements of the research problems and research questions which were re-define through the pilot study to provide a background for the archival analysis.

4.2.2 The Relevance of Archival Analysis in this Research

The emphasis of the importance of the archival analysis in social science research has spanned across the emerging research domains including but not limited to IS security management. In analysing history of the archival thought, Cook (1997) notes that the role of archival analysis in IS security management research has changed from being supplementary references to becoming a reliable research approach for research knowledge enthusiasts. Archival records have become a potential research value for micro-analyses of the creator's key functions, activities, programmes and interactions with the business environments. Archival analysis can be used to get a holistic picture of an on-going phenomenon, and could be used to address research issues of change over time. Hadfield (2010) suggest that archival research provides multiple levels of evidence – individual, community, organisation and social, to any given research problem. It provides detailed, objective, and subjective description of events from multiple viewpoints. These attributes of archival analysis make it possible for researchers to provide more complete evidence than other forms of data collection.

Archival analysis enables the researcher to make use of the archival data that have been processed by statistical expertise. It reduces the chances of flaws in the data analysis and increases the validity of the collated data (Gabriel, 1990). For instance, Durkheim's (1966) study on 'change on women's status; he compared the institutionalisation and suicide rates' by using the United Nations data collected from 45 nations. As it used in this research, majority of the data collated for the analysis were garnered from the libraries and internet archives of British Retail Consortium (BRC), UK police records, financial service authority, security exchange commission and other business regulators. Archival analysis availed the researcher opportunity to establish a timely and sequential historical records that answer research questions of the cases under study. It saves the researcher the resources. Archival analysis enables the research to gather reliable data on what participant might not be comfortable with in some critical line of inquiry (Holt, and Fawcett and Rabinowitz, 2012); as it is in this research that deals with the information security issues.

4.2.3 The Relevance of Participant Observation in this Research

As defined by Bradbury and Reasons (2001) participant observation is the whole family of approaches to the inquiry which includes action-oriented, grounded in experience and participative. Participant observation requires the researcher to be into research situation, bring about change while monitoring the ensuing research results.

Kemmis and McTaggart (2000) note that participant observation centres on a 'spiral of reflective cycles' of planning a change, acting and observing the process and consequences of change, reflecting on the emerging processes, and then re-planning. They describe participant observation research with seven features as; a social processes critical, emancipatory, practical and collaborative, participatory, aims to transform both theory and practice. Galliers and Land (1987) and Galliers (1990) agree that participant observation is a suitable qualitative research which can be used in the field of IS security for studying complex, multivariate, and real world phenomena. Bakerville and Pries-Heje (1999) agree with Galliers and Land that participant observation is vital for the study of information system development issues like security because of its orientation toward change. This issue of change forms the basis for the use of participant in this study a relevant tool of inquiry for a 'technological shift' as business operations in the online retail migrates into the digital realm. This relevance of participant observation in this study was suggested by Davenport and Short (1990) and Klein and Hirschheim (1989). They suggest that participant observation can be viewed as an enabling facilitator of change and result of a change, which is both the business organisation imperative an emergent perspective.

Although there is relevance for the use of participant observation in the information systems security research, few researchers have used it as a research method. Several researchers (e.g. Mathiassen *et al.,* 1991; Puhakainen and Siponen, 2010) argue that sparse literature on the use of participant observation in the information systems security research has been attributed to the reason that it is often eclipsed by traditional social science research methodologies like case studies and sampling. Galliers (1990) and Orlikowski and Baroudi, (1991) agree with this argument and suggest that few of the top quality IS security research published is conducted with participant observation. Bakersville and Pries-Heje (1999) studied the use of participant observation in the context of the IS security research; and asked why few researchers have adopted the approach? In answering this question, they attributed the reason to common assumption by researchers that theory evolution of research would occur as result of rigorous problem formulation, not of the research approach.

Bakersville and Pries-Heje study agrees with Glaser and Strauss (1967) suggestions that participant observation can be adopted for rigorous theory formulation and that the use of theory formulation steps in participant observation improve research rigour which involves merging some of the techniques of grounded theory.

This research adheres to the suggestions of Glaser and Strauss (1967) and Bakersville and Pries-Heje (1999) and adopted participant observation to evaluate the application of the role-based framework as an extended theory of preventing IIDTRC. Since the key aspect of participant observation is the role it plays in the theory formulation, this research provides a framework as a theory that based its formulation on research results from participant observation cycles. Following the ensuing evaluation of the outcomes of each cycle, the researcher reinforced the theoretical framework, modify or withdraw to reflect the realities of the action-taking. Hence, participatory observation is chosen as a viable option for this research to achieve the research aim.

4.2.4 The Relevance of Moderate and Active Participant Observation

In the context of achieving this research aim and considering that a participant observation is a complex qualitative research approach with many components, moderate participation and active participant observation were chosen. This is in adherence to the suggestion of Spradley (1980) that the first thing a researcher must do after deciding to conduct participant observation is to decide what kind of observer to be. Moderate participant observation and active participant observation are among the other four components of participant observation: Non-Participatory, Passive Participation, Moderate Participation, Active Participation and Complete Participation; suggested by Dewalt and Dewalt and Waylant (1998) and Spradley (1980). They explained that moderate participant observation enables the researcher to maintain a balance between 'insider' and 'outsider' roles. As this is envisaged in this researcher, assuming the role of moderate participant would allow the researcher to be involved as well to be detached in order to remain objective in monitoring the IIDTRC prevention practices of retail management.

Similarly, assuming the role of an active participant will enable the researcher to be more involved in the population. Though Dewalt, Dewalt and Waylant (1998) suggest that there might be the risk of 'going native' as the observer strives for an in-depth understanding of the population studied, this approach would enable the researcher to fully embrace the skills and customs for the sake of complete comprehension of the research problem (Emerson and Fretz and Shaw, 2001). And this strategy and approach are necessary for this current research which requires the understanding of the complex issues of IIDTRC and peculiar practices of management in the online retail business environment.

4.2.5 The Relevance of Triangulation in this Research

As described by Stake (2000), triangulation is a process of using multiple perceptions to clarify meaning, verifying the repeatability of an observation or interpretation. Triangulation is employed in this research to improve the validity and reduce the likelihood of misinterpretation of empirical data (Nair and Riege, 1996). Kaplan and Duchon (1988) suggest that triangulation of qualitative data in IS research increases validity. In agreement with Kaplan and Duchon (1988), Carson and Gilmore (1996) argue that collecting different kinds of data by different methods from different sources provides a wider range of coverage that may result in a fuller picture of the systems units under study. This argument forms the basis for the relevance of triangulation in this study – to allow the use of multiple methods that would increase the robustness of results which can be strengthened through the cross-validation achieved when different kinds and sources of data converge and are found congruent.

Denzin and Lincoln (2005) described topologies of triangulation which include data, between methods, investigator, methodological, multiple and within-methods. Kelle (2001) described triangulation into complementarity and trigonometrical; Deacon, Bryman and Fenton (1998) expressed it into planned and unplanned; whereas Morse (1991) categorised triangulation as simultaneous and sequential triangulation. This research employed these topologies of triangulations. For instance, the evaluation case study provides the between methods triangulation – semi-structured and participant observation; whereas analysis of this case studies involve simultaneous triangulation – the content analysis and coding.

For the overall analysis, the research uses both theoretical and methodological triangulation. As suggested by Danziger and Kraemer (1991), the IS research project that involves fieldwork such as qualitative case study, as it is in this research has always provided complementary sources of sound evidence. With both approaches providing valid research findings, the case study is noted for its high discoverability attributes in research.

4.3 Summary of the Research Philosophy and Methodology

This chapter has provided the concepts of the research activities – the philosophy of the research, the research methodology and research designs. These analyses were done to provide the overview of the case study protocols and how the research questions and objectives dictate the research approaches.

In summary, this section has provided the background of how this research project is framed by a constructivist and interpretivist paradigms so that the selected research methodology had to be compatible with and reflect these philosophical views. While the interpretivist concept enabled the researcher to affirm the significance of the participants' knowledge of internal identity theft-related crimes in the online retail, the constructivist concept enabled the researcher to make assumption about much complex behaviour of the subjects being studied. And that this knowledge 'subjects' possess has important consequences for how behaviour or actions are interpreted.

This study required that all participants shared not only in the construction of developing knowledge but also had an understanding of each other's objectives of participation and underlying reasons for participation so that these could be taken into account in the data analysis and interpretation. Hence, the interpretivist paradigm adopted in this study has provided the researcher with deeper shared understanding through its perspectives of embedded process of reporting and discussion at all stages of the research design, research finding and research story.

This chapter has laid the foundation for the data collation and the analyses that would be discussed in chapter 5 and chapter 6 respectively.

CHAPTER 5

DATA COLLECTION

5.1 Introduction

As discussed the chapter 4, the archival analysis, semi-structured interview and participatory observation were chosen for the data collection in the selected retail companies. Yin (1994) suggests that archival analysis, semi-structured interviews and participant observation are main sources of evidence in case study research design. These methods were designed as discussed in this chapter to provide answers to this research questions. This chapter provides details of selected case background, the case selections, the data collection protocols, the practicalities and dilemmas encountered. In addition, the practicalities of these methods provide a comprehensive view of the collected data that inform findings derived from this study that will be discussed in chapter 6.

5.2 Background of Case Study: UK Online Retail

The UK retail sector is chosen for two major reasons. First, the UK Online Retailing is a £9.4 billion industry, accounting for approximately 5 per cent of Gross Domestic Product, with more than 10 per cent of all employment (Gambin *et al.,* 2012). UK Online Retailing comprises Beauty and Personal Care Internet Retailing, Consumer Electronics, Consumer Healthcare Internet Retailing, Media Products Internet Retailing, and Other Internet Retailing. According to Centre for Retail Research, 2008-2012, the UK Online retailing combine with Germany and France accounted for 71 per cent of European online sales (Nicklin *et al.*, 2013). Thus, the experience of UK's retail sector can be taken as an important indicator of experiences of other Organisation for Economic Co-operation and Development (OECD) countries.

Second, long before the Internet, the UK Online Retailing has been one of the early adopters of electronic trading operations. The UK online retailing has a long tradition of Internet-based focus. The trend for the digitisation of the online retail operation and their business transaction using credit/debit cards necessitates sharing of the consumers' sensitive personal identifiable data. However, Internet offers the UK retailers opportunities to match this trend but not without the problems of internal identity theft related crimes (IIDTRC) to contend with.

In socio-economic terms, this industry shapes the livelihood of UK consumers and affects online consumers' ability to respond to e-commerce challenges like identity theft. The UK retail sector has been characterised as one of the sectors where most of the consumers are vulnerable to IIDTRC with less investment in the prevention (National Fraud Authority Report, 2013; Forrester and Seeburger, 2013)

Therefore, the UK retail sector therefore provides a unique setting to understand nature of internal identity theft related crimes prevention in e-business.

5.3 Case Selection and Design

This study took open consultations with a number of retail companies since the choice of organisations is vital to case study design. In total, four retail companies (*RetailGroup*, *Xtail*, *Ytail* and *Ztail* for anonymity) were selected; *RetailGroup* was selected for a semi-structured interview while *Xtail*, *Ytail* and *Ztail* for the participant observation. The selection is based on three factors. First, gathering data from the case study with multiple firms allowed the research to use a "case-replication" methodology to test the applicability of the findings across cases (Yin 1984).

Second, the companies' business culture, size (medium to large) and ethics, and their experiences in the field of e-commerce and e-tailing are recognised as the most common business strategies the retail industry across globe adopts. Third, the retail companies were willing facilitators and participants in this research endeavour and have ensured the researcher that they will be open to provide the data required and also interested in the feedback from the research—a key practical consideration when embarking on field-based research (Pettigrew, 1990).

In addition, to the above factors, Denzin and Lincoln (2005) noted that it is vital to choose research cases on the basis of opportunities to gain accessibility and to learn. Marshall and Rossman (1999) also suggest the need for a rich mix of people, processes, interactions and structures of interest to be present in a choice of cases under study. The selected companies possessing the distinctive and well-structured business culture and practices provide the researcher great opportunity to gain access to these firms by getting in contacts with the top management (Wilson, 2010). The companies engage in series of 21st century modern methods of retailing business operation. The companies are renowned retail corporations in the United Kingdom. Most of them were established in the 2000s and has acquired many corporate retail brands.

Therefore, based on the chosen retail companies meeting these three criteria, their branch offices situated in the north-west of UK were selected. The location of these offices suited the choice of researcher's research strategy as regards to the base university[10]. This enables the researcher to get access to the research participants with ease on time and at reduced costs (Hakim, 2000). It enabled the researcher to have access to more data; as it is conventional research, the more data, the better. It also allowed the researcher time for conducting interview and analysis of collated data.

5.3.1 Archival Analysis Case Design

For the archival analysis, the retail companies selected comprise the business organisations which allow consumers to directly buy goods or services from a seller over the Internet using a web browser. These include retail corporations which use business-to-business (B2B) online shopping and processing of services. The cases analyses were extended to the banking sectors because of the direct link to the online retail companies operations with the online banking. The retail companies collaborate with banking sectors in processing of the consumers identities and authorisation of the payment for the complete online shopping operation. To answer the research question of the nature of internal identity theft related crimes (IIDTRC) in the online retail, an analysis was based on the UK archival resources from 2007 to 2013.

The analysis includes IIDTRC empirical research reports from the website portals, digital libraries, newspapers, magazines and/or organisation's archived newsletters, annual reports, special reports and other electronic resources. The archival resources were underpinned by the annotated business reports by British Retail Consortium and UK Financial Service Authority. It extends the past research works by analysing a different time period related IIDTRC media reports (shown in table 29 below). It critically analysed the contents of the reports, the reporters/authors perspectives, and contexts of the IIDTRC incidents. In retrieving the data from these sources, a search was conducted for articles and reports that contain but are not limited to the following terms in abstract, keywords and title: identity theft, insider theft, data leakages, data breaches, identity theft: propagation, detection, prevention; and business information security, information systems security management, and software security.

[10] University of Central Lancashire, Preston UK

Organisation	Archive Materials
CIFAS	Research Reports on Staff Fraud (2009-2011 editions); Staff Fraudscape: Depicting the UK's staff fraud landscape (2010); Fraudscape: Depicting the UK's fraud landscape (2009 to 2010); Digital Thieves: A special Report on Online Fraud (2010); The Internal Betrayal: a special report on beating the growing threat of Staff Fraud (2010).
British Retail Consortium (BRC)	Articles on Staff Fraud (2008-2011); BRC Reports (2007-2011 editions); BRC Online archives: Press Releases (2008-2011), Company News (2008-2011); Media Analysis (2008-2011); and Speeches (2008-2011).
Biz/ed (www.bized.ac.uk)	Research Reports: News & Media Releases Archive (2008-2011 editions), Primary Business and Management information in UK focus: Management Structure, Code of Conducts & Ethics; and Interpretation of the Mission Statement
Biz Info.Serv	UK Business information, research statistics, surveys and reports.
Public Media	Local & National Newspapers in UK; ThisDay Newspaper, DailMail Newspaper, The Sun Newspaper, etc.; BBC Online, Sky News Online.
National Staff Dismissal Register (NSDR)	Database of employers to share details of dismissed staff but not convicted in the criminal courts for offences of dishonesty related to IIDTRC. It aims at the retail industry, in particular, created in March 2009 by Action against Business Crime, a consortium formed by Home Office and British Retail Consortium.
ABCP Archive	Association of Business Crime Partnerships (ABCP) is an independent not-for-profit organisation working with business (retailers) crime reduction partnerships (BCRPs), police, police and other agencies to help business reduce the impact of crime on them.
UK Data	Collection of UK digital data in social sciences and humanities.
NFA Archive	This collates substantial documents and reports from National Fraud Authority in relation to Annual Fraud Indicator, UK Fraud Prevention Service – CIFAS and Commercial Victimisation Survey Report.
The Police Central e-Crime Unit (PCeU)	The Unit was established in September 2008, works in conjunction with the Metropolitan Police Computer Crime Unit of Scotland Yard. This provides national investigation report of the most serious cybercrime incidents in the UK businesses.

Table 29: Archive Materials

To establish the relevance of the articles returned by the search, each of the articles was reviewed in full. It was critically guided by the research objectives, and the key issues that are imperative for the prevention of IIDTRC in the online retail. The dataset-like criminal profile was created from an in-depth analysis of data contained the archives. The profile describes common types of internal identity theft related crimes cases with names of individuals who have caught engaging in IIDTRC. It covers their age, gender, job title, motivation, how caught and lessons learnt. The design of this analysis is detailed in chapter 6 to reflect a diversity of IIDTRC as they relate to online retail.

5.3.2 Semi-Structured Interview Case Design

For the semi-structured interview, *RetailGroup* (renamed for anonymity) was selected. It was selected for semi-structured interview because it operates as a multi-brand comprises of five retail companies. This multi-brand structure was selected to a provide a comprehensive understanding of the research problem: the nature of identity theft related crimes (IIDTRC) in *RetailGroup*, status quo of IIDTRC prevention framework used by *RetailGroup*, the extent of how attributes of the role-based framework fit in the *RetailGroup*, and the evaluation of how the *RetailGroup* security management interact.

5.3.2.1 RetailGroup and Security Management Structure

RetailGroup is a leading online retailer within the British Isles, thanks to the on-going restructuring and modernisation of the companies. Their traditional paper-based and phone-in orders system have been superseded by modern e-commerce and e-tailing technology. The companies' experience in the field of e-commerce and e-tailing development in the UK is indicated by the fact that they have successfully acquired many brand names, and amalgamated the brands into its shopping networks, warehouses and call centres. The companies' controls assets valued in excess of billion worth of revenue annually. Collectively the companies have over 11 million employees that handle over five millions of customers' data with over 20 million calls and over 55 million items per day. This research was centred on the prevention practices of the *RetailGroup*'s data security and crime prevention management (figure 14 *RetailGroup* Security management structure).

The typical management structure is headed by group operation director who plays a leading role in the integration of the businesses and is responsible for all of the group operations, including warehousing, contact centres, security, shipping, web and catalogue production, transport/logistics and the group's extensive infrastructure and sites. The management role under the group operation director is group security director, on whom other four management roles (head of security support, head of security operations, training manager, and the information security) directly report to.

The head of security support is responsible for the security intelligence unit, internal frauds/crimes and investigation reports, security of workers, vetting and physical security administration. The head of security operation is responsible for the security of the control room and the companies' regional loss prevention. The information security team comprises other four management roles: technical security, data security compliance, technical security specialists, and the compliance. *RetailGroup* outsources to renowned IT security companies which include IBM and RSA to complement their IT security and support.

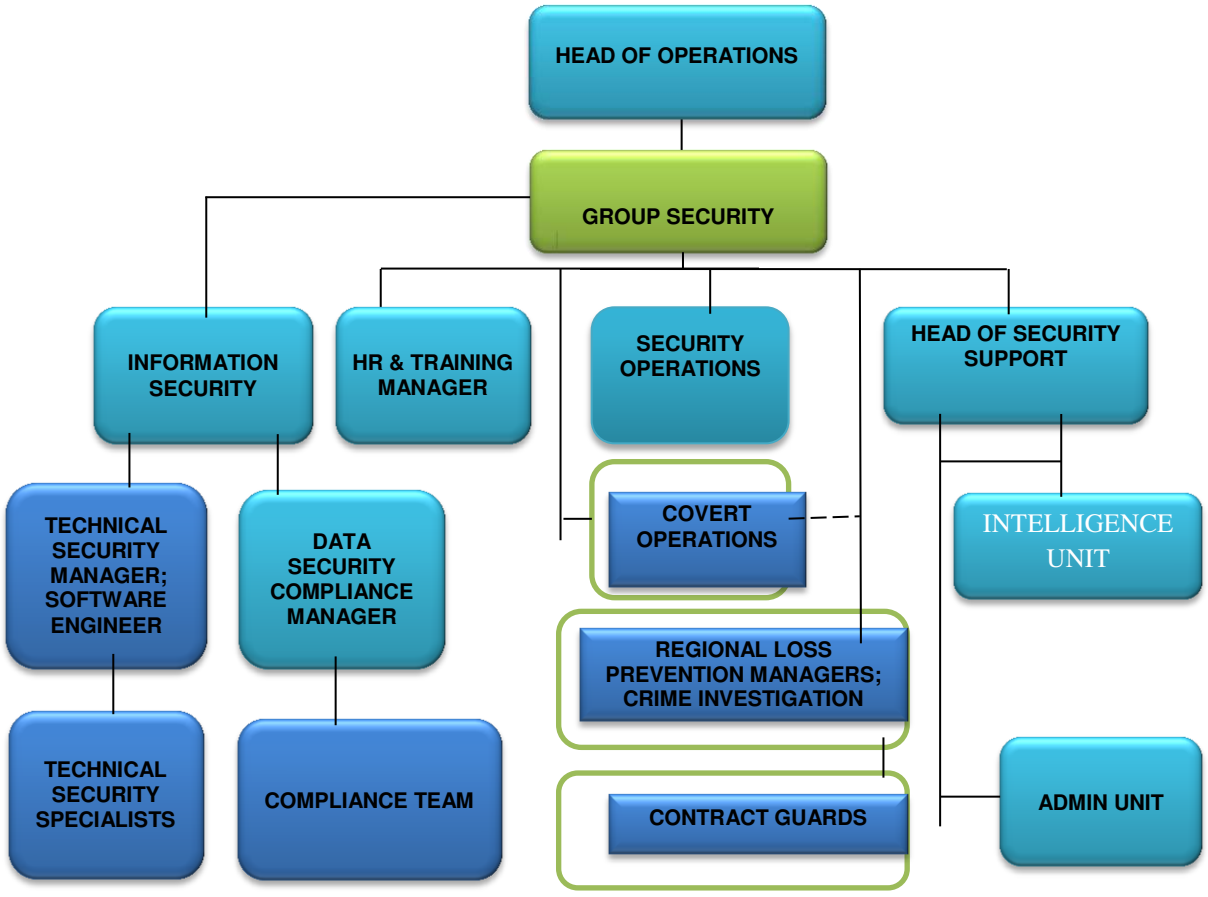


Figure 13: Retail Security Management Structure

5.3.2.2 Access to Data in RetailGroup

At the outset of interview data collection, the researcher made a formal agreement with the *RetailGroup* by signing an Ethic Approval Form from the University of Central Lancashire. This was to ensure that the research was carried out in accordance with the University Code of Conduct. Since the ethics of the research is important and 'a must do' in this research, it provides informed consent to the research participants and also respected their right to privacy. The researcher made primary contact with the top management of the companies. Though, *RetailGroup* did not provide an easy access to some of their top security managers, the researcher had to use this researcher sponsor as the gatekeeper to access the key top manager.

As a result of this issue of access to participants, the interview data collected did not provide cross-section knowledge of their roles in data security and IIDTRC prevention. There were differences in the level of understanding of the security and crime prevention roles between the management that are directly involved with the *RetailGroup* security roles. To address the issue of bias due to lack of cross-section of interviewees, the researcher undertook telephone interviews. This was used to complement some cases where the face-to-face interviews were proved logistically impracticable.

In total twelve semi-structured interview sessions were conducted, with nine sessions conducted through face to face and three by telephone. The technique to have an option of either face-to-face or telephone semi-structured interview enabled the researcher to obtain the optimum cooperation of the participants (McCrossan, 1991). As a multi-method of data collection, this technique availed the opportunities to monitor and to respond to visual cues of the interviewees, and build a relevant contextual analysis (Burton, 2000). The researcher ensured that interviewees were not given their own opinion that was not relevant to the lines of enquiry. This was used to reduce bias related to what Weick (1995) described as the two entities of interviewees' behaviour in organisation – the interviewee as him/herself and the interviewee as a representative of the *RetailGroup* under study.

5.3.2.3 Data Collection in RetailGroup

A semi-structured interview was used to clarify key IIDTRC prevention issues and evaluate the application of the proposed role-based framework in *RetailGroup*. It has allowed the researcher to access to participants' view and interpretations of actions and events (Walsham, 1995). Although the flexibility and open-ended nature of unstructured interview would have been helpful, it was not adopted it was not used in this research. This is because of its weak generalisability. Instead, the semi-structured availed the researcher the best access to participants' views and interpretation of actions and events. As it applied to this research, Easterby-Smith, Torpe and Jackson (2012) suggests that semi-structured interviews are appropriate where the interviewee context is unclear, the step-by-step logic of situations is not clear, or the subject matter is confidential or sensitive as it in this research.

5.3.2.4 Interview Participants in RetailGroup

Since interview is suitable where a researcher is able to observe behaviour or feelings (Bryman and Bell, 2011), the researcher utilised this approach as a form of conversation with 12 selected participants to generate research data (Denzin and Lincoln, 2011). The roles of the 12 participants from the *RetailGroup* are as shown in table 30 below. The 12 participant were interviewed from September 2011 to April 2012. All the participants have worked for *RetailGroup* for least 5 years. They were aware of the importance of the data security and need for IIDTRC prevention and have been involved in number of IIDTRC prevention initiatives in the *RetailGroup*.

In several cases, multiple interviews were conducted to reduce the bias and to increase the consistency and validity of the data (Yin, 1984). It enabled the researcher to ensure the uniformity and consistency in the data that included opinions, facts, and unexpected insights. Each interview lasted from a minimum of 45 minutes to a maximum of 1hour 30 minutes depending on the participant.

The interviews were conducted in the respective participant business premises. This enabled the researcher to get information about data environment, business operations, the security tools and resources. While conducting interviews, the researcher followed a technique of "theoretical sampling" (Strauss and Corbin, 1998). If the researcher identified a set of factors and parameters that led to a certain outcome, the researcher would then direct his enquiries to determine the change in the outcome, given a change in the set of parameters.

This enabled the researcher to ascertain a better understanding of the causes of the crimes incidents. For instance, the researcher often investigated whether the observed cause of a certain type of employees' crime incident was due to lack of clear role given to the internal data security management team or not adhering to the security policy. In this manner, he could investigate whether an observed outcome had occurred irrespective of the security tools in place, or it was due to the unique software security loopholes that exist on the platform of which crime prevention team operates.

Professional Role	**Management Position**	**Mode of Interview**
IT Security	Head of security support	Face to Face
Crimes Prevention	Head of crimes investigation	Face to Face
Data Compliance	Group Data Compliance	Face to Face
Crimes prevention	Head of Crimes prevention	Face to Face
Operations	Head of Security Operations	Face to Face
IT Security	Technical security specialists	Telephone
Human Resources	Training Manager	Face to Face
IT Security	Software Engineer	Face to Face
IT Security	Compliance team manager	Telephone
IT security	Technical Security Specialist	Face to Face
Crimes prevention	Regional Loss Prevention	Telephone
Human Resources	Head of Human Resources	Face to Face

Table 30: Interview Participant's Management Positions

5.3.2.5 Interview Protocol in RetailGroup

A set of protocols was employed to enable the researcher to design a set of guiding questions for the semi-structured interview. The guiding questions helped the research to provide answers questions based on Role-Based Framework attributes. The interview questions were focused on the development of the coherent cases of the crimes within the companies, placing their experiences of IIDTRC in context, encouraging integration of their organisations' IIDTRC incidents and recovery experiences, and risk management and IIDTRC preventive control measures in place to curb the crimes. The questions were used to explore the roles of the various management (as listed in table 20 above), the companies IT security structures, IT management processes, and their capabilities as regards to internal data security and IIDTRC prevention. Table 31 below detailed questions used for the interview sessions.

Question Tags		Research Questions	Research Objectives
Q1 **Introductory Question**		What are the nature (causes and methods of propagation) of IIDTRC in your organisation? (Newman, 1984; Reith, 1956).	To provide an account of the nature of IIDTRC, noting the socio-economic impact, the causes, and the methods of propagation of these crimes in a distinctive context from those in UK online retail.
Q2 **Q3**	**I** **II**	What are the IIDTRC prevention measure/strategies in your organisation? (Prosch, 2009; Boyle, *et a.l,* 2007; Collins, 2003) What are your roles/ responsibilities as part of the management team in preventing IIDTRC? (Lawrence, Suddaby and Leca, 2009; Savirimuthu and Savirimuthu, 2007; Cabri *et al*., 2006).	To identify and develop a systematic IIDTRC prevention framework capable of synthesizing a clear set of role-based recommendations among the relevant management.
Q4 **Q5** **Q6**	**III** **IV** **V**	Do you collaborate with other management roles in implementing IIDTRC strategies? (Shah and Okeke, 2011; Salinger *et al.*, 2008; Kardell, 2007). What are the management (s) issues you encounter in preventing IIDTRC as an individual or as a team? (Hinds, 2007). What factors affect collaborative roles in the IIDTRC prevention; what evaluation approaches used? (Jendly *et al*., 2010).	To evaluate the applicability of the framework by examining the working of retail management from the perspectives of organisational role sharing backgrounds.

Question Tags	Research Questions
I → II	What is your most effective IIDTRC prevention strategy, and why? (Lacey and Cuganesan, 2005)
I → III	How do your management roles help or hinder effective IIDTRC prevention in practice? (Collins, 2006)
II → III	How does management understand and share IIDTRC prevention roles and what skills and expertise do they need for IIDTRC prevention? (Hurst, 2010)
II → IV	Are there any strategic IIDTRC prevention processes in place to support your management roles? (E.g. Can you describe how you interact with other security units in a typical IIDTRC incident; detection, investigation to the prosecution of the case (Homel, 2010; Anderson and Tresidder, 2008).
III → V	What practices and techniques are used to evaluate/implement management roles in relation to IIDTRC prevention and internal data security (Homel *et al.*, 2007)?
IV → V	What are the challenges of IIDTRC prevention as an individual or team in practice? (Boyle *et al.*, 2007).

Table 31: Interview Questions

In table 31, the Roman numerals (I to V) are used to depict the related Role-base Framework attributes discussed in chapter 3. The questions at the outset of the interview covered variety of the company's issues involving the nature of IIDTRC prevention extending to causes of IIDTRC, the roles and responsibilities of a crime prevention management, the possible challenges of crime prevention management, and possible areas of improvement for effective data security. By considering the boxes and linkages of the framework and how they are supported in the literature review and archival analysis, subsequent questions were derived. While flexibility was allowed by the researcher in the course of the interview sessions, these research questions were used as the topic guide for the enquiry. The similar approach of the interview sessions was adopted for the participant observation research discussed below. Though, in those cases the convergent interview was used.

5.3.3 Participant Observation Cases Design

For the participant observation, three retail companies *Xtail*, *Ytail* and *Ztail* (for anonymity) were selected to complement the data collected from the *RetailGroup*. The selected cases were designed to examine application of the role-based framework and to confirm the hypothesis from the literature review which underpins the theoretical framework discussed in chapter 3 that:

- *Collaboration of the management has impact on the management roles (IS/T and crime prevention) in prevention of IIDTRC; and*
- *The collaboration of management roles has an impact on the implementation of tools required for the prevention of IIDTRC.*

Thus, it provided the answers to the research questions 2a and 2b in the chapter 1 of this study respectively:

- *To what extent do the attributes of the framework influence the internal identity theft related crimes prevention practices?*

- *To what extent do the IS management influence the effectiveness of identity theft related crimes prevention framework implementation?*

In particular, moderate and active approaches to the participant observation were used to study the roles of Information Systems Audit (ISA) management on prevention of internal identity theft related crimes (IIDTRC). Data collection was carried out through an active participant observation in *Xtail* and *Ytail*; and moderate participant observation with *Ztail*. In all the cases, the data collected from the observation was triangulated with a daily reflective journal, field notes and convergent interview data. The choice of moderate and active participant observation in this study was to maintain the flexibility of this study and to provide a comprehensive investigation of the cases. Unlike the active participant observation, which has the advantage of allowing the research to make considerable time for planning and simultaneous delivery of case study, the moderate participant observation allowed the researcher carry out comprehensive case study with limited amount of preparation and time (Emerson, Fretz, and Shaw, 2001). The application of the latter was valuable because this study was conducted within a short period of time. In addition, considering the structure of Ph.D. programme that allows a minimum amount of time for data collection. Moderate participant observation also allowed the research to collect rich and directly observed data for relatively low costs and minimum time.

Collectively, the used of active and moderate approaches of participant observation enabled the research to explore the practicalities of fieldwork in both familiar and unfamiliar business settings of *Xtail*, *Ytail* and *Ztail* in their operational environments.

Xtail: *Xtail* is one of the largest retail companies in the UK and operates in many countries across Asia, Europe, and US. It has been established for more than a century evolving with the trend in retailing operations. It accrues approximate annual revenue of multi-billion pounds. *Xtail* has many fasciae with numerous stores spread across UK. It employs more than quarter a million staff that handles millions of club card customers' data with over hundreds of thousands of online orders per week. Its major products are grocery, clothing, and home wares. It also handles financial services such as credit and extended warranty services.

Ytail: Similarly, *Ytail* is one of the top 50 UK retail companies with a multi-billion pounds worth of annual revenue. It has been in operation for many decades with many fasciae and many stores across UK. Its employees, circa thousands, handle millions of customers' data per week either online or over the phone. *Ytail*'s major business is financial services and household item sales.

Ztail: The third company, *Ztail* shares a similar business operation culture with *Xtail* and *Ytail*. Though with lesser annual revenue, it handles thousands of the customers' data.

Since these companies have extended their wider retail business operation from financial services to the sourcing business operation. Their business operations include mail order trading via several catalogues and websites. Their financial services are made up of other divisions such as fraud prevention, operational risk, insurance, and underwriting.

These divisions are made to offer millions of customers a variety of products including credit, extended warranty, insurance products and tailored ways to pay including buy now pay later. Their IT security, financial services team and the crimes prevention, in particular,do not only ensure that all the companies' retailing operation are fully compliant and regulated by the UK Financial Services Authority; they are committed to protecting the company assets and customers data.

5.3.3.1 Locating Xtail, Ytail and Ztail

The audited companies - *Xtail*, *Ytail*, and *Ztail* were located in the cities with the high density of online retail companies in the Northwest of United Kingdom. The choice of these companies was motivated by the rationale discussed in the section 5.3 above. *Xtail* and *Ytail* were contacted when the researcher was working as a member of Information Security Research Group (ISRG) at the University of Central Lancashire. Then, the ISRG was working on research project identity theft prevention with number of retail companies across Northwest of UK. Working as a part-time research assistant with ISRG over a few months of weekly visits, the researcher established rapport and trust between the research facilitators and sponsors. With the support of research sponsors, snowball sampling technique (suggested by Mars, 1982) was applied to locate and contact *Xtail*, *Ytail* and *Ztail*. Thus, through the research sponsors, *Ytail* and *Ztail* were recruited. After a number of contacts to explain the scope of this research to *Xtail*, *Ytail* and *Ztail*, it transpired that they were interested in this research topic. In that, they accepted an 'outsider' into their companies to review the conduct of role their information system audit (ISA) management. This discovery about their interest in the scope of this research demanded that a more cross-sectional recruitment approach to be adopted than case-controlled approach.

Instead of selecting only ISA professionals as originally envisaged, the available and convenient individuals were selected from the mainstream management population. This strategy allowed the study to be conducted in its natural setting without the intervention of the research requesting individuals with specific characteristics. The research anticipated that adopting a case-controlled approach of requesting for the research participants with specific characteristics might introduce bias and affect the reliability of this research. For the *Ztail* moderate participative observation, the main concern was to obtain a representative of various roles and settings in which the management worked. In this case, the sample selection was less problematic because the researcher relied on 'colleagues' from sponsoring companies who helped to select individuals that cooperated with the researcher. Consequently, the researchers inevitably encountered various situations in *Xtail*, *Ytail*, and *Ztail*, including attending meetings, business departments' visits, and telephone requests. The researcher was either a participant-as-observer for the case of *Xtail* and *Ytail*, and/or an observer-as-participant for the cases of *Ztail*. Thus, the researcher placed more central role on participation than on observation for *Xtail* and *Ytail*, and as observer-as-participant, more emphasis was placed on observation than on participation (Gold, 1969).

5.3.3.2 Challenges of Access, Ethics and Withdrawal in Xtail, Ytail and Ztail

This section reflects on the ethical issues in relation to access and withdrawal challenges of participant observation fieldwork the researcher experienced in *Xtail, Ytail* and *Ztail*. By assuming a participant observer role, the researcher was able to observe the professional roles and practices of the security management in the *Xtail, Ytail* and *Ztail*. However, the researcher has to put up with ethical issues in relation to the challenges of access and withdrawal in this research concealment. In doing so, the researcher was able to fulfil the ethical obligation by adjusting to overt and covert role as the research situations and circumstances required. Abiding by the ethical rules motivated participants to express their information systems audit roles regarding the prevention of internal identity theft-related crimes in the *Xtail*, *Ytail* and *Ztail*. In addition, by adjusting the level of researcher's involvement, participating in ISA of *Xtail* and *Ytail* as an insider and observing in *Ztail* as an outsider, the researcher was able to adapt and respond to ethical dilemmas in *Xtail*, *Ytail* and *Ztail.*

The researcher conducted the fieldwork in *Xtail, Ytail* and *Ztail* bearing in mind that ethics of participant observation should be cautiously addressed to the sensitivity of this research topic – prevention of internal identity theft related crimes, the vulnerability of the participants – IT security and crime prevention management, and the dynamism of membership role of the researcher in the fieldwork. Undertaking this research as a participant observer, the researcher was careful at the outset of the fieldwork and was prepared to use the strategy of trust and professional orientation to adapt to the potential issues of getting access to and withdrawal from *Xtail*, *Ytail* and *Ztail*.

Trust aspect of access and withdrawal to *Xtail, Ytail* and *Ztail*

Participant observation cases – *Xtail, Ytail and Ztail,* as they are in this research required the fundamental need for trust between the researcher as an observer and case companies. Rousseau *et al.,* (1998) defined research trust as a, *'psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another'* (Twyman, Harvey and Harries (2008, p.112). Sonnenwald (2003) conceptualised the need for and building of trust in organisational research by examining cognitive and affective trust. Sonnenwald (2003, p.3) defines cognitive trust as a '*judgements about a person's ability to execute a certain task effectively*' while affective trust is an '*interpersonal bonds among individuals and institutions'.*

Both concepts of trust have relevance in the context of this research. Access to the research subjects – *Xtail*, *Ytail* and *Ztail* was somewhat easy because of the trust between the researcher and the participants. It was eased by the fact that the researcher and this research gatekeeper not only worked for the same company (research sponsor), they shared common concerns and interests in collecting of research information.

From the outset of the active participant observation study in the *Xtail* and *Ytail*, the researcher had to develop affective and cognitive trust with the gatekeeper to ease access to the *Xtail* and *Ytail*. Unlike the moderate participant observation study in the *Ztail*, where there were few common concerns and interests in access and provision of information. This observation reflects suggestion of Pettigrew (1999a, b) that research subjects of moderate participant observation do not view access to information provision in the same discrete way as subjects of active participant observation (*Xtail* and *Ytail*) and business professional might.

Adhering to Pettigrew's (1999a, b) suggestion, trust was developed to nurture how to access the information from the *Xtail*, *Ytail* and *Ztail*. Emphasis was given on the process of building trust and relationship with the *Xtail*, *Ytail* and *Ztail* as well as on collection of information from them, reflecting what O'Neill (2002, p.76) has suggested that researchers should: *'place trust...because we can trace specific bits of information and specific undertakings to particular sources on whose veracity and reliability we can run some checks. Well-placed trust grows out of active inquiry rather than blind acceptance…'*

Interestingly, the challenge of getting access to the moderate participant observation in the *Ztail* accorded with the process of active inquiry suggest by O'Neill (2002), in which the *Ztail* granted access to the researcher with a few moderate enquiries and restrained hesitations. In addition, this experience is in accordance with suggestion by Keirns *et al.,* (2013) that ability for a researcher to use trust to gain access to hesitant research subjects is a vital strength of participant observation. In this current research, participant observation had allowed the researcher to gain access, however the challenge, to investigate the behaviour that would have been normally restricted from both researchers and the outsiders in the *Xtail*, *Ytail* and *Ztail*.

Hence, the researcher maintained the trust by working with the gatekeeper (research sponsor) in a way that the trust was not damaged by access and withdrawal of the researcher from the case companies.

Professional aspects of access and withdrawal to *Xtail, Ytail and Ztail*

In the *Xtail* and *Ytail* settings, a professional relation between the researcher and the selected Information Security Audit (ISA) management made access somewhat easier. The professional relationship was built on the fact that the researcher has an in-depth knowledge of information security auditing. This knowledge was gathered through the researcher's experience while working as a research assistant in the field of identity theft prevention (areas of IT security) at the base university. Researchers (e.g. Wax, 1979; Dewalt and Dewalt, 2002; Ladson-Billings, 2003) suggest that professional orientation is one of the personal characteristics among others – age, gender and race, that affects the researcher-participant relationship in field researcher.

Age, gender and race did not matter in this research, but professional orientation did. As an experienced IT security professional, the researcher was able to acculturate with security terms of the security audit, which to some extent ease access to ISA management in both *Xtail* and *Ytail*. Consequently, the researcher was not perceived as a potential security threat to *Xtail* and *Ytail*. Arantzamendi *et al.*, (2012) suggest that professional relationship between the researcher/observer and participants establishes a good level of communication that would improve the confidence between both parties. This suggestion of relationship between observer and participants reflects what Tojar (2006) called reactivity – the impact of the presence of the researcher on participants' behaviour, and that professional relationship between observer and research lessens reactivity. Taylor and Bogdan (2000) agree and suggest that establishing a good professional relationship with research subjects in the course of ethnographic research, as it is in this case, lessen reactivity.

This professional relationship advantage lent support to the researcher's position to understand security audit roles and practices of the management in *Xtail* and *Ytail* regarding IIDTRC prevention. Thus, enables the researcher to observe participant in their natural setting which also fosters a climate of trust. In the *Ztail* setting, access to ISA management (for moderate participant observation) was more difficult as was the withdrawal. Unlike the active observation in *Xtail* and *Ytail*, there was complication of access to the *Ztail* setting in the initial phase of the fieldwork but access restriction was lessened through the use of Ethical Letter from the base university and Letter of Introduction from this research sponsor. The combination of the trust and professional relationship, however, did not grant easier access to *Xtail*, *Ytail* and *Ztail* as did by the use of Ethical Letter and Letter of Introduction.

Ethical Letter aspect of access and withdrawal to *Xtail, Ytail* and *Ztail*

In addition to the assistance the researcher gained from the retail company that sponsored this research, two strategies were drawn upon to gain access to *Xtail*, *Ytail* and *Ztail*. First, an Ethical Letter, as evidence of support from the base university was presented to *Xtail*, *Ytail* and *Ztail*. Li (2008) advised that ethnographic researchers should prepare themselves to conduct an ethical study. And that ethical preparation enables researchers to eliminate and avoid ethical dilemmas regarding the sensitivity of the research that might restrict their access to the research subjects. In line with the Li (2008) suggestion, other researchers (Punch, 2000; Murphy and Dingwall, 2002; Lather, 2004) advocate that it important for participant observer to draw a clear line between the ethics and the politics of their ethnographic fieldwork. They noted that researchers should emphasise and supply both ethical evidence and their research ground in order to contest against social prejudice in relation to research access.

From this standpoint, the researcher felt that in order to conduct an ethical study that guarantees unrestricted access, the Ethical Letter from the base university was given to *Xtail*, *Ytail* and *Ztail*. The presentation of the Ethical Letter prepared the researcher both psychologically and technically for the unexpected regarding the access the *Xtail*, *Ytail* and *Ztail* (Li, 2008).

Secondly, the data compliance manager of the company that sponsored this research sent a Letter of Introduction (introducing the researcher and research aim and objectives) to the management of *Xtail*, *Ytail* and *Ztail*. Gold (1959) suggests that prior introduction of the researcher to the research subjects by the research sponsor makes the researcher/observer to gain access to situation in which researcher can collect information or learn about the organisation, requisite daily roles successfully. Such introduction, as utilised in this context, helped the researcher to gain access without being seen as an outsider in the *Xtail*, *Ytail* and *Ztail*. The researcher was permitted to share not only in work activities with the ISA management but also in the intimate the culture of the companies regarding the use of security auditing in preventing internal identity theft related crimes. However, *Xtail* and *Ytail* expressed concern about the confidentiality of the data to be collected from their companies, even with continuous confidentiality and anonymity assurance.

Consequentially, perhaps because of this concern, a copy of previous IIDTRC case report of *Xtail* and *Ytail* that was requested by the researcher was not given after several attempts were made.

This restricted access to their IIDTRC case report reflects Li's (2007) suggestion that research participants might have some reservation regarding releasing some sensitive information due to some objections from their cultural or organisational background.

This issue of restricted access to the *Xtail* and *Ytail* was a concern to the Research Ethics Committee of the base university and research sponsor. And they had to review the application of this research and clarified the detail assurance on the issue of this research confidentiality and anonymity. The Research Ethics Committee laid more emphasis on the protection of the companies' sensitive in information in relation to data privacy and security. Paradoxically, although access was difficult in the *Xtail* and *Ytail* even with the Ethical letter and the support of this research sponsor, withdrawal proved to be even more difficult in both, although the sponsor's affiliation with the base university guaranteed the *Xtail* and *Ytail* data protection and privacy after the conclusion of this research.

For the moderate participant observation in *Ztail*, there were fewer requirements at the outset of the study. Apparently, there was a less critical review of the research protocol for the Ethical Approval as the researcher was not directly involved. The researcher was accepted not just as an outsider but as an employee from this researcher sponsor. The strategy of access to *Ztail* was suggested by de Laine (2000) that a possible mode of entry in sensitive organisational research (IT security in this case) is to move from the position of an outsider to that of an insider. This suggestion was applied by the researcher and having worked with the research sponsors and then has legitimate access. Having anticipated that acquiring ethical approval and that finding companies to study and that gaining their acceptance would take time.

In addition, the researcher has anticipated that the problem of 'sustained access to research subjects' is a widely recounted issues in typical ethnographic studies (e.g. Wilson and Streatifield, 1997; Eager and Oppenheim, 1996; de Laine, 2000; Hammersley and Atkinson, 2007). For instance, Wilson and Streatfield (1977) noted that participants feel less obtrusive in the presence of observer during interview meetings than in the case of participant observation, reflecting that interview avails sustained access than participant observation. In agreement with the Wilson and Streatfield (1977), Eager and Oppenheim (1996) suggest that research participants when working at their desks found the presence of the researcher rather unsettling, though the participants had established access permission with the researcher at the research outset.

Gatekeeper aspect of access and withdrawal to *Xtail, Ytail* and *Ztail*

At the outset of this study, the research sponsor was the gatekeeper for access to both *Xtail* and *Xtail* and *Ztail*. The sponsor as the gatekeeper was made aware of the underlying intention of the researcher - the research aim and objectives. At all times, the intention has to be reminded to the gatekeeper, ISA team and external auditors that this study is primary to the researcher's function as an information security auditor. Onwuegbuzie *et al.*, (2009) advise that providing the research participants with clear information on the research problem, its aim and objectives and research questions is very important in participant observation. In addition, Van Maanen (1988) points that clear explanation of the importance of the research motivates the participants to be open, explicit in expressing their behaviours and interact freely with observer without holding back on their experiences.

While the role of information system auditor assumed by the researcher granted the initial entry to the *Xtail*, *Ytail* and *Ztail*, it did not guarantee continued/sustained access or acceptance by the management of *Xtail* and *Ytail* or the respective audit team. Equally it didn't assure the complete and continued membership of the researcher with the management in each situation. For instance, the head of IT security who was one of the three members of the audit team in *Xtail* rejected the request of the researcher to participate in the company's webserver auditing. As it would have been in any IT security setting, the researcher has anticipated such rejection perhaps because of the sensitivity of security in relation to data privacy of the company.

As the overt approach did not work in the auditing of *Xtail*'s web server, the level of the researcher's involvement was adjusted from active to moderate (Spradley, 1980). The research still took part in observing the web server auditing, but intentionally limited personal involvement and expertise in the audit procedure. Instead of actively involving personal interactions or substantial conversations with auditors, the researcher mainly jotted notes about the auditing activities. In other words, the researcher primarily assumed a covert observer in the web server auditing, a peripheral professional role and a detached insider. Alder and Alder (1987; 2000) suggest that peripheral membership role enables the observer to be reflexive and be prepared for any exigency. This adjustment not only helped the researcher to avoid ethical dilemmas experienced at the outset of seeking for access, but also equipped the researcher with much-needed psychological strength to participate in conducting ISA in the *Xtail* and *Ytail* as an insider and observed as an outsider.

Membership role aspect of access and withdrawal to *Xtail, Ytail* and *Ztail*

The researcher's role as company's staff, as a security auditor in the cases of *Xtail* and *Ytail* made permission for the study easier to grant. As the researcher was not only bound by the Research Ethics agreement but also with *Xtail* and *Ytail* companies' staff code of conduct and confidentiality. For the moderate participative observation in *Ztail*, the management granted permission on the understanding that they would be observed to obtain a better understanding of their collaborative management roles in the prevention of IIDTRC. Researchers (e.g Spradley, 1980; Bernard, 2006) suggest that participant observers who acculturated themselves with the roles of the participants have better chances to conduct and produce valid research outcomes.

However, the ISA management of *Ztail* were not shown the observation sheets used for field notes, for each identified IT security issues, the level of the seriousness of the security issue, in case these developments biased their normal roles and behaviour. Although, the results of the ISA and sources of the results were not reported to them; how and what would be done with analysis of the collected audit results were revealed to them. In addition, how their roles and behaviour impact the results were not discussed with them.

However, there was a dilemma in conducting the participant observation; the trust that was built throughout the studies enabled the researcher to gather data that answered the research questions – 2a and 2b, stated above. The finding that the selected cases – *Xtail*, *Ytail* and *Ztail*, themselves viewed the sharing of their companies' information as vital as granting access to the cases, establishing and maintaining relationship with the researcher is no doubt made the research more challenging to undertake. Notwithstanding, adhering and familiarising with suggestions by the ethnographic literature explored above, the researcher found it challenging to convince and lessen the participants concerns and interests about dilemmas in sharing their companies sensitive security information.

5.3.3.3 Modelling Participant Observation in Xtail, Ytail and Ztail

The researcher applied the Snyder model of action research (suggested by Dick, 2002) to extend how the role-based framework (RBF) attributes are applied as it related to roles of Information Security Audit (ISA) in real business context of *Xtail*, *Ytail* and *Ztail*. This model was applied to collect data for analysis of the collaborated ISA approach and independent (internal or external) security audit practices.

In addition, the research evaluated the impact of the approaches on audit performance and processes to identify their implications for good practice in the prevention of IIDTRC. This research strategy enabled the researcher to achieve the aim of examining the robustness of RBF and how they work in practices.

In particular, the researcher adopted evaluation participatory action research and adapted the Snyder Process as recommended by Dick (2002); and elaborated on the importance of the Snyder Evaluation Model in evaluation participatory action research. The Snyder model comprises of the three evaluation sequences: process, outcome and short-cycle. The use of these sequences which have been applied by other researchers (Dick, 2001; Irani, 2002) enabled the researcher to address research issues that would contribute to change in organisational practices (Dick, 2001). For instance Irani, (2002) applied the Snyder Model to understand how activities and resources accomplish immediate effects, ideals and targets, in order to achieve the research aim. The outcome evaluation and short-cycle evaluation enable researchers to develop performance indicators and set up feedback mechanisms respectively. These suggestions by Snyder Model are utilised in this research to monitor the effects of the research activities and effectiveness of the ISA practices.

The Snyder Model which is based on systems concepts and number of processes – inputs (resources), transformations (activities) and the outputs levels – immediate effects, targets and ideal, enabled the researcher to address the research problems in sequences. It also enabled the researcher to analyse, as discussed next in detail, how IS security audit tools, resources and activities accomplish the immediate effect, targets and ideals.

In addition, the researcher used the outcome evaluation to develop practices and processes and to estimate the attributes of RBF with respect to ISA approaches – joint/collaborated and independent. This process enabled the researcher to monitor the immediate effect of RBF attributes as it relates IS security audit initiatives in the companies under study. By setting up feedback mechanisms, this creates an immediate update ISA system that hastens the audit activities. The audit feedback analysis and interpretation made the audit process easier to manage and reduces the number of visits and research cost. This strategy which is similar to total quality management (TQM), that was suggested by Ward, Anand and Tatikonda (2010), builds on the integrative and interpretive philosophy of management for improving the quality processes as related to time and cost (Ahire, 1997). In addition, this design enabled the researcher to bridge the gap between the theories and real ISA practices (Jorgensen, 1989).

5.3.3.4 Participant Observation Protocol in Xtail, Ytail and Ztail

Based on the Snyder evaluation steps discussed above, the study of *Xtail*, *Ytail* and *Ztail* involved data collection procedures from two sources: observation and convergent interviews. The data collected from these sources was built with the requirements of ISO 19011:2011 assessment tools and guidelines, previous Information Security Audit (ISA) reports of *Xtail*, *Ytail* and *Ztail*. The researcher built the evaluation of the company's ISA practices based on the recommendation and requirements of ISO 19011:2011. As an assessment tool, ISO 19011:2011 is applicable to all companies that need to conduct IS security auditing either jointly or independently (external and internal) and manage an IS security audit programme. The researcher assumed that the auditors (and audit team) have the required competence needed to perform IS security audit with impartial, objective, systematic and in a well-documented form.

ISO 19011:2011 also required that IS security auditors have discipline-specific, sector-specific knowledge and skills in order to carry out ISA, generate ISA findings and conclusions. The definitions below summarises key audit terms adopted based on ISO 19011:2011 guides and principles.

IS security Audit (ISA): An evidence gathering process was used to evaluate how well IS security audit criteria were being met to prevent IIDTRC risk in selected companies (*Xtail*, *Ytail*, and *Ztail*) under review. IIDTRC risk is the chance that IIDTRC will occur or negative deviation from the objective of IIDTRC prevention. Three types of IS security audit are first party, second party and the third party. In this research practices of the first and second party were evaluated. The first party involves the use of internal auditors to confirm (self-declaration) the company's IS security compliance, while the second party is done by customers (regulators or party that has formal interest in a company) on their behalf. The third party are performed by the independent organisations (certification bodies or registrars).

Information Security Auditor: A person who carries out IS security audits and uses collective evidence for ISA evaluation to determine whether the audit criteria are met.

ISA Auditee: An organisation or company (in this research the *Xtail*, *Ytail*, *Ztail*) that were audited. Other terms related to auditee are audit client – internal and external audit client, the former could either be the auditee or audit program manager, whereas the latter could be other parties (regulators, customers) that have a legal/contractual right to carry out an IS security audit.

ISA criteria: These are policies, procedures and requirements used as a yardstick for the audit evidence – how well the criteria are being implemented, applied and followed. Audit evidence (objective) can be records and factual statements that prove that something is true/false, expressed either qualitatively or quantitatively. Other terms related to audit criteria are: conformity (compliance) and nonconformity (non-compliance); while the former indicates that criteria are met, and the latter indicates that the criteria are not met.

ISA Plan: This describes or specifies how the auditor and audit team carry out ISA activities to achieve the audit objectives. It involves prioritising the audit programmes (set of arrangements such as setting objectives, assigning responsibilities, allocating resources and monitoring performance) to conform with available resources – cost, personnel, time, logistics, etc.

ISA Scope: A statement which specifies boundary and the focus of an audit programme. It involves defining organisation units, the locations, activities and processes to be covered.

ISA Team: It is made up of two or more security auditors, audit trainees, observers (in some cases it involves technical experts – IT support, software engineer, inventory manager, etc.). In this study the researcher was part of the audit team as an observer – we did not perform audit functions that demand a high level of IS security audit competence. Technical experts support and provide expertise and information about the companies being audited.

ISA Findings: This is the summary of whether the audit programme is either compliance (pass) or noncompliance (fail). It identifies the improvement opportunities, recommendations and practices that result from audit evidence.

Audit Conclusions: This is done after the audit findings and audit objectives have been considered. It involves final decisions and recommendations.

The researcher adopted the requirement of ISO 19011:2011 to ensure that the audit programme and evaluation processes were free from bias. In addition, to address the internal validity of the research findings, the ISO 19011:2011 was used to complement the convergent interviews. This strategy was used to check and resolve discrepancies in the collated data. Consequently, as suggested by Jick (1979), this approach ensures that data collection protocol converged with the recommendations and requirements of ISO 19011:2011 principles. Table 32 summarises the steps of the data collection protocol.

Stages	Procedures	Activities of the Audit Programme	Duration
1	Introduction and preparation	Scheduling ISA appointment with the key contact persons. Requests for the companies' IS and ethics policies (The researcher gave the auditee 3 weeks of notice prior to visiting for the fieldwork). Going through their relevant information system policies and business ethics. Collection of necessary security clearance and requirements from the UK Data Protection Act (DPA). These activities provided the sound understanding of the companies under review and DPA clearance was used as an authority to have access to all IS resources. The researcher explored the ISA security analysis and risk management: checked the companies IS management to determine the size and prioritise the key areas for the review.	Approx. 3 Weeks
2	Policy and document review	In most cases the researcher treated the companies IS policies and IS configurations as threats. The review the selected cases' data protection policies to explore how the policies define the use of IS resources and who has access to them.	1 week from the start of the auditing
3	Convergent interview	The researcher had questions and answers sessions with the selected audit team (as shown in table 23) and discussed the usage patterns of the IS security resources, the IS security policy awareness among the staff members and how they are communicated across the organisation. The researcher also attempted to ascertain vital information on what vital IS security tools, strategies, and the process used; and how management views the ISA. This approach was to avoid research bias as it relates to ISA implementation perceptions from management. In addition, the researcher asked an open-ended question related to key IS of the auditee for contingency and reporting incidents, software and hardware inventories, etc.	Approx. 20 to 30 minutes during the auditing of the selected case.

Stages	Procedures	Activities of the Audit Programme	Duration
4	Observation and technical investigation	This step involves: full code review of websites to locate possible developers' errors (buffer over/underflows, poor coding, backdoors, etc.) which might lead to potential IIDTRC threat/risks; and the system logs to explore the usage patterns and potential vulnerabilities. The 12 major IS Security Priority Areas investigated are: Data Protection Act Documents, Data Disposal Policy, Business Continuity Policy, Data Field Protection, Physical Security, Personnel/Employee Monitoring Procedures, Websites and Network Security, Infrastructure (Laptops, Logical Access, and Servers) Security, PCI and Ofcom Compliance Documents.	Approx. 3 weeks with at least 3 visits to the selected case
5	Investigation and Data Review	This stage involved the researcher going through the audit document to update the observation; and also made noted of critical issues to be written in detail in the audit report. The collated electronic version of the observation report was documented reference in research analysis.	Approx. one week from completion of Step 5
6	Documentation and writing up	After each visit, the audit reports would be documented by the researcher. The document was updated regularly up to the last audit appointment of the respective companies. The researcher evaluated observation with the last IS audit report of the auditee. All the documents collated were reviewed and summarised for the final audit report – detailed recommendations and a timeframe for the implementation. The summary of the report was done according to the priority of the security risk issues and graded using colour coding for the level of associated risks – green (no risk), amber (low risk), red (high risk).	Approx. one day
7	Presentation and feedback report	The presentation of the report involved the management staff. The expected time (depending on the level of risk) for the implementation of recommendations was specified.	Approx. 1 day
8	Postreview and updates	This stage involves reviewing the implementation. In some cases (if the implementation involves low-risk issues or documentation) it was done through conference calls.	Approx. 3 weeks

Table 32: Information security audit procedural stages

The designed ISA procedures encompass the 8 key stages. Each of the steps, as shown in the table 32 above, provides the description of the actions taken by the researcher. The stages as shown in the table above were followed by the exchange of auditee contacts and audit schedules. Each of the procedures was applied to the three selected companies (*Xtail*, *Ytail*, and *Ztail*) except in some cases where the duration for completion of the audit activities depends on the quantity of documents and size of the company. In case situations, these stages were not followed sequentially. For instance, in some situation during observation the convergent interview was conducted before, during or after the Technical Investigation to clarify some issues prior to or after the investigation. The practicalities of the observation in these cases are discussed in the next section.

5.3.3.5 Practicalities of the Participant Observation in Xtail, Ytail and Ztail

With the support of this research sponsor, a purposive sampling strategy was adopted to select *Xtail* and *Ytail*. An in-depth case study of *Xtail* and *Ytail* and observational approaches were adopted to enable the researcher to investigate the real life picture. In the term used by Kluckhohn (1940) he states that participant observation;

> *'is the conscious and systematic sharing, in so far as circumstances permit, in the life activities, and on occasions in the interests and effects of a group of persons' (Rock 1979, p.187).*

This statement interestingly describes the situation of observation in both cases – *Xtail* and *Ytail*. It was through shared understanding built up over time by the researcher with *Xtail* and *Ytail* can practical knowledge be learned during personal encounter by researcher and management (Smith, 1988). In this study, a regular contact time was maintained by the researcher to acquire the practical knowledge of the IIDTRC prevention practices and to identify the personal interaction between management and researcher. To avoid security and privacy issues or linguistic barriers that might have hindered communication in those situations, the researcher placed greater reliance on symbols including body languages, facial expressions, management gestures as well as their interaction in both *Xtail* and *Ytail* settings.

In essence, the use of participant observation approach allowed the researcher to monitor these issues while studying the participants.

The cases of *Xtail* and *Ytail* involved working with selected management as shown in table 33 and active participant observation was used for both settings. The line between the covert and overt nature of the active participant observation in *Xtail* and *Ytail* was blurred due to the overwhelming nature of the audit protocols. It was difficult for the researcher to be introduced at every stage of the ISA without interrupting the auditing procedures. In the same vein, moderate participant observation was used in *Ztail*. In this setting, the nature of observation was overt. There was detail introduction for both the researcher and the subject before the ISA procedure.

Cases	**Management Position**	**Auditing Approach**	**Approx. Auditing Duration**	
			Investigation	**Implementation**
Xtail	Head of IT Support IS Security Auditor	Joint party (internal + external + Researcher)	3 days	4 days
Ytail	Operations Manager Account General Manager	Second party (External Only + Researcher)	7 days	10 days
Ztail	Customer Acct Manager Internal ISA	First party (Internal Only + Researcher)	5 days	8 days

Table 33: Management Positions of ISA Team and Approximate Audit Duration

Table 33 shows the respective companies (*Xtail*, *Ytail*, and *Ztail*) with the participant's management position and approximated auditing duration. Active participant observation involved categories of participants: *Xtail* and *Ytail* (audited companies), internal auditors and external auditors who have direct contact with the *Xtail* and *Ytail*. In these cases, the researcher assumed dual overt and covert roles. The researcher was one of the external auditors and at the same time an observer. With the researcher's experience of IT security, the researcher participated in auditing of the both the *Xtail* and *Ytail* security tools (server, firewalls, and web application updates).

Due to the researcher's involvement with the audit activities, the researcher was accepted as '*one of*' the external auditors. And on those situations, the research facilitator overlooked to introduce the researcher to *Xtail* and *Ytail*. But in some situations where the researcher was introduced, the researcher was accepted as an observer and/or researcher.

Although studies on 'workings' of Information Systems Audit (ISA) have been carried by researchers (Dittenhofer, Ramaoorti, Ziegefuss and Evans, 2010; Steinbart *et al*., 2011; Wallace, Lin and Cefaratti, 2011) they were conducted through interviews (e.g. Steinbart *et al*., 2011) or quantitative survey (e.g. Wallace, Lin and Cefaratti, 2011).

A few or no research in this area had adopted a dual role as an insider approach. By becoming 'an IS auditor' enabled the researcher to see reality of the everyday world of the *Xtail* and *Ytail* practices of preventing IIDTRC. It also allowed the researcher to interpret meanings and symbols underpinning the companies' daily collaborative role and interactive responsibilities of the ISA management (Lee and Newby, 1989).

5.3.3.6 Convergent Interview Protocol in Xtail, Ytail, and Ztail

The researcher engaged the Information Systems Audit participants with convergent interviews via open-ended questions. The questions were developed as the interviews were ensuing. The open-ended questions were used for an in-depth examination of the ISA related organisational issues since this research is interested in the findings that might be used and contribute to theory building (Perry and Rao, 2003; Dick, 2001). Spradley (1980) suggests observation technique offers a more direct and objective view of the subject behaviour while interviews provide indirect means of validating the observed information. In total, there were 6 participants, two security auditors from each of the selected companies.

In most cases, interviews were conducted in the auditee office. In some cases, the interviews were carried out during the auditing transient time (switching times from one activity to another) or after completion of the audit programme for the day. The participants were interviewed on the key research questions summarised in table 34 below.

	Convergent Interview Questions	Rationale
1	What is your attitude as a part of your company's management to Information Security Audit (ISA)? What changes (if any) have you witnessed over past years in your company?	ISO 19011:2011 requires that Information Security Audit should be a priority of the management in business organisations; Steinbart *et al*., (2011) and Dean *et al.,* (2012) suggest that the review of Information Systems and the relationship between Information Security Auditors and management should be done regularly.
2	Which information security audit frameworks(s) exist in your company or used in your company (if any)? What IS security auditing processes are important, and the critical success factors for control? What are the ISA measure/strategies in your company in relation to IIDTRC prevention? (Prosch, 2009; Boyle, *et al.,* 2007; Collins, 2003).	From the literature review in chapter Chapter 2 above, several researchers (e.g. Collins, 2003; Homel *et al*., 2007; Boyle, *et al.,* 2007; Anderson and Tresidder, 2008; Prosch, 2009; Homel, 2010) suggest the need for frameworks to guide policy; or the existence of an internal data protection/control framework; Lacey and Cuganesan (2005) suggest need for the management to understands most effective IIDTRC prevention strategy.
3	Which information/data protection policies/regulations/standards (e.g. Data Protection Act, Ofcom, PCI) are most important to you?	Data Protection Act and Ofcom require the need for businesses that holds consumers data to be compliance with regulations/standards of data protection; PCI requires that that businesses need to comply with standards and policies that promote effectiveness and efficiency of security audit services.
4	What is the status quo of the ISA staff in your company? How many IT staffers are dedicated to your security auditing and how often is it done per annum? What evaluation processes or approaches, if any, are used? (Jendly *et al.*, 2010).	Cilli (2003) suggests the need for businesses to answer questions related to fundamental IS security issue such as performance measurement (how well is the IS security auditing enhancing business requirement?)
5	How would you characterise the working relationship between the Information Security Audit staff and the IT security staff? What are your roles/responsibilities as part of ISA management in preventing IIDTRC?	From the literature in chapter 2 several researchers (e.g. Cabri *et al*., 2006; Savirimuthu and Savirimuthu, 2007; Kardell, 2007; Salinger *et al.*, 2008; Lawrence, Suddaby and Leca, 2009; Hurst, 2010; Shah and Okeke, 2011) suggest the need for management to understand and share IIDTRC prevention roles, skills and expertise.

Table 34: Convergent Interview Questions

After auditing visits which take several days; in some cases weeks depending on the auditing approach – either joint or independent, scheduled short-cycle feedbacks were conducted followed via e-mails and conference calls. This was done to enable the researcher to monitor the impact of the audit and implementation of the notable data security issues as they relate to the prevention of IIDTRC. The convergent interview with the IT security staff and auditors complemented the observation of the interaction and collaboration of the external auditors and the management of *Xtail*, *Ytail* and *Ztail*. An inductive, grounded theory (Glaser and Strauss, 1967) was applied in the analysis of the field notes and transcripts. The categories and themes extracted from the data analysis were reviewed and manually analysed throughout the audit process based on the proposition of role-based framework. This approach allowed the emergence of categories and themes from the data for analysis of role-based framework that was discussed in chapter 3. The results of the analysis are discussed in the next chapter.

5.4 Summary of Data Collection and Case Study Design

This chapter has presented the description of the data collection methods. It has the practicalities of data collection protocols. It also described how the principle of data collection models and approaches was applied in the case studies. In summary, since the aim of this research is to provide a framework to prevent internal identity theft-related crimes in the online retail companies; this chapter has presented;

- *the design of archival analysis for understanding the nature of IIDTRC,*
- *the design of case studies via interview and participant observation for evaluation of the role-based framework,*

In addition, the designs and practicalities of these data collection methods provided a comprehensive view of the how this research data was collected to inform the result that is discussed in chapter 6.

CHAPTER 6

DATA ANALYSIS AND RESULTS

6.1 Introduction

There are a number of approaches in the literature for analysing qualitative data, common suggested approaches are archival analysis, content analysis, experimental and testing programmes. These analytical approaches answer to *what works*, *for whom*, *in what circumstances*, and *why* (Pawson and Tilley, 1997). In dealing with the task of an appropriate analysis for this research, archival analysis and content analysis approaches have been selected. They were considered to satisfy the needs of this research based on the background reading of the role-based framework (RBF) evaluation methods discussed in Section 3.4.

Based on the qualitative research methodology that has been discussed in the Chapter 2, archival analysis and content analysis were suggested as the appropriate for archival data and interview data respectively. These approaches appeared as the most appropriate for evaluating the theoretical framework and defending the outcome of this research. The purpose is to manage the validation of the research outcome via a cross-case analysis, in an attempt to confirm, prove or disprove the propositions. Hence, this research makes use of archival analysis and content analysis to break down the collected data into manageable pieces in such a way to meet the research issues and objectives as well as to provide answers to research questions.

The rest of this chapter contains four sections. Section 6.2 provides the results of the archival data analysis. It provides the answers to what the nature of IIDTRC is like in a UK online retail companies and relate businesses such as banking sector. 6.3 provide the results of the data collected from selected case companies: *RetailGroup*, *Xtail*, *Ytail*, and *Ztail*. Nvivo 10 software aided the content analysis of the data collected via semi-structured interview while manual content analysis was used for the data from the participant observation cases. Some of the cases involved transcription, coding of recorded voices, documentation of field notes, and model representations. This strategy enables the research to explore further on the areas of interests of the extended attributes of the role-based framework. 6.4 triangulate the findings as cross cases analysis to examine how the themes of the collated data interplay with the RBF attributes and 6.5 provides the summary of this chapter.

6.2 Analysis of Archival Data: Internal Identity Theft Related Crimes Cases

The number of Identity Theft Related Crimes (IIDTRC) cases recorded by fraud prevention bodies and law enforcement agencies had risen by nearly by 60 per cent in 5 years in England and Wales. According to Office of National Statistics (ONS) (2014) more than 230, 000 cases of IIDTRC and employees related frauds were recorded in England and Wales from January to June 2014. This figure represents 59 per cent rise in 5 years and more than a fifth on the previous 12 months. Online retail and banking sectors recorded a further 316,000 cases of IIDTRC and related employees frauds. In total over 12 million cases of IIDTRC and related employees fraud cases were recorded in the 12 months period, although the ONS (2014) noted that these figures recorded across business sectors may have overlapped. These reports suggest that prevalence nature of IIDTRC in UK e-business sectors. The rise in these crimes in both retail and banking sectors may have been due to the nature of online business operation of these sectors, which carry less risk of being caught. Norman Baker, the UK crime prevention minister and Jack Dromey, the UK shadow policing minister, noted that identity theft related frauds have increased by 21 per cent because much of these online crimes go unreported.

This analysis was done based on the empirical data of individuals who have been caught perpetrated internal identity theft related crimes (IIDTRC) in the UK. The case of the individuals analysed is not limited to UK online retail sector. It has included some cases of other sectors (e.g. banking) because of the multi-faceted operational nature of the retail sector business through credit/debit cards (See the Appendix 2 for case examples from the Banking Sector). These cases were directly or indirectly involved with online retail and banking sectors due to the relationships both sector share in their business operations. The background of this relationship has been discussed in Chapter 5 above.

Although this section defines IIDTRC in the context of the online retail sector, this definition is extended to other sectors as illegal compromise of any information system, network, data, which identify the victim as the statutory owner under UK Data Protection Act, 1998. The victims, in this case, are the retail companies in relation to their customer. The compromise involves act where the suspect/perpetrator has or used legitimate access to IS, network, or data comprised. The suspect/perpetrator includes current/former employees of the victim retail companies, current/former consultant/contractor/partners.

This section deals with behind the scenes analysis of actual cases of internal identity theft related crimes (IIDTRC), revealing what went wrong and illustrating how the crimes were perpetrated; even the most unsuspecting operation. It provides the in-depth understanding of the nature of IIDTRC in the victim companies. The aim of this research to provide a comprehensive framework for prevention of IIDTRC may not be achieved if this research does not provide real time data of where and how the perpetrators operate.

If a research fails to know the companies operation's greatest risks and vulnerabilities are, (Haley, 2013) suggested, such research may not have enough knowledge to develop and implement a realistic anti-fraud and crimes prevention framework. Adhering to this suggestion by Haley (2013), this section introduces a number of examples of individuals who have been caught attempted to and/or engaged in internal identity theft related crimes and frauds. A majority of the cases analysed below were extracted from archives of the National Staff Dismissal Register, the Association of Business Crime Partnerships, and National Fraud Authority. Case analysis IIDTRC perpetrators cover their age (at the time of the fraud), gender, job title, description of the nature of the fraud (attempt), motivation, how caught and lessons learnt. The internal identity theft related crimes analysed in this research have been categorised into corporate identity theft related crimes and personal identity theft related crimes. Though full discussion on concepts of these categories has been reviewed in Section 2.4.5 of Chapter 2, it is important to revisit those explanations in this section;

Corporate Identity Theft Related Crimes: The impersonation of a company for financial or commercial gain. Fraudsters steal your company's identity and/or financial information and use it to purchase goods and services, obtain information or access facilities in the company's name. The common schemes include unauthorised alteration to company data/ modification of company payment instructions.

Personal Identity Theft Related Crimes: The impersonation of another person for financial gain. Fraudsters steal personal identity and/or financial information and use it to purchase goods and services or access facilities in someone's name; it is the use of a false identity or another person's identity to obtain goods, money or services by deception. This often involves the use of stolen, counterfeit or forged documents such as passports, driving licences and credit cards. The common schemes include Application Fraud/Account Takeover, Present (Current) Address Fraud and Account Withdrawal.

Some of the corporate identity theft related crimes cases analysed were collected from the public domain (see Appendix 2). In those cases, the names of the fraudsters were retained. In the cases that were not in the public domain, no identifying information is given and all the names have been changed to protect the individuals' privacy.

Case #1 Personal Identity Theft Related Crimes in the Private Domain: Account Takeover

Name	'Jane'
Age	32
Gender	Female
Job title	Cashier
Nature of fraud	'Jane' stole numerous Credit Cards that were left by customers in a rush after shopping. She used the card to make purchases from her own company's online portal. After several weeks the crime was not discovered, she continued to use the debit card to make more purchases from other online retail portals.
Motivation	**Opportunity:** She had an opportunity and she took it. She believed that everyone in the shop could have done the same. **Self-Justification:** 'Jane's' main justification was that she didn't think she was doing something wrong. She had the opportunity and made use of it. She thought that everyone would have done the same internally and that could justify her fraud as the norm. **An absence of monitoring system such as CCTV cameras:** Since there is no surveillance in place to check the employees internal shop activities, 'Jane' was convinced that she would never be caught.
How she was caught	In the similar situation of stealing the customer's credit card whenever it was left at the shop after shopping, this particular woman came in the next day as she had realised she had left her card behind, checked with her bank and found out it had already been used. 'Jane's' company called the police and she got arrested.
Lessons learned	**Fraudsters' perception of barriers and lack of defence against crimes:** Due 'Jane's' company lack of a verification procedure, she found it easy to bypass their website defences. It was easy for her to defraud e-commerce sites that have no identity verification or shared fraud alert data which would have tripped her up.

Lessons learned	If there was identity checks such as name and address, a complete identification of the individual could have emerged which would flag up negative fraud alerts in the customers' databases. **Failure of the Credit Card Companies to Report the Fraud:** It was easy for Jane to continue her fraudulent scheme because the credit card companies fail to report the fraud to card owner. **Customers Negligence:** In addition, there was negligence of most online retail customers to check their spending regularly with their banks.

Table 35: Case #1 Identity Theft Related Crimes: Account Takeover

Case #2 Personal Identity Theft Related Crimes in the Private Domain:

Personal Identifiable Data Theft from Employer's Database.

Name	'Smith'
Age	24
Gender	Male
Job title	Software Engineer
Nature of fraud	'Smith' gathers customers' personal identifiable information from his Company's information systems and sold them to his customer in the 'black market'.
Motivation	Expertise: 'Smith' has used his technical skills to exploit the information systems of his employer and stole information for his personal gains. The Demand for the Personal Information by Fraudsters: The huge demand for the online credit/debit card details has created 'hot product' perception for both 'Smith' and his customers.
How he was caught	'Smith' hack activities on the information systems were revealed by the biannual information audit. The trails of how he log into the company's information database were analysed and he was arrested. During his fraud investigation, it was revealed that numerous customers' card details were found on his personal laptop and some hidden websites that he has been using to sell the stolen card details.
Lessons learned	The absence of Regular information security audit in 'Smith's' company allowed his lots of time to perpetrate his fraud without having been caught.

Lessons learned	There is no effective security system in place to prevent 'Smith' from hacking his employer's information systems though if it exists he would have used his IT skills to manoeuvre it. High-security surveillance should be placed on the software engineers because they could pose a huge security threat to companies. Knowing which job tasks create the greatest internal fraud risks should be an important component of any manager's preventative strategies.

Table 36: Case #2 Personal IDTRC: Data Theft from Employer's Database.

Case #3 Personal Identity Theft Related Crimes in the Private Domain: Personal Identifiable Data Disclosure

Name	'Ceri'
Age	29
Gender	Female
Job title	Credit Card Issuance Officer
Nature of fraud	An Employee Embezzled £310,698 from an Employer. 'Ceri' manipulated a payroll and credit card scheme that led to her embezzling £310,698 from her small business employer over a period of five years
Motivation	Boost of Annual Salary: She was using the stolen money to boost her annual salary. Family Pressure: 'Ceri' used her Employer's account to pay for daughter's three credit card bills totalled more than £15,000.
How she was caught	Numerous calls from customers, complaining about non-payment. The calls sparked an investigation that was reported to the local police. During the course of the investigation, the investigation team discovered that 'Ceri' had a record of the improper use of a credit card.
Lessons learned	Past behaviour is an excellent predictor of future behaviour. A thorough background check can provide valuable information, especially when a candidate is applying for a position of trust. Such an investigation would likely have prevented 'Ceri' hiring. The revelation of fraudulent activities by 'Ceri' started when the customers complained about not receiving their payments for services/goods rendered. This employer made a most positive move by not allowing such complaints to be investigated by the employee charged with processing those transactions.

Table 37: Case #3 Personal Identity Theft Related Crimes: Data Disclosure

Case *#4* Personal Identity Theft Related Crimes in the Private Domain: Account Withdrawal

Name	'Kathy'
Age	47
Gender	Female
Job title	Accountant
Nature of fraud	An accounting clerk wrote 137 retail companies' contract payment cheque valued at £1.4 million and deposited them into her personal account. This trusted employee was given the authority to prepare cheques without proper internal safeguards and reasonable management oversight.
Motivation	**No segregation of duties/Working alone:** This individual could prepare and issue cheques without being scrutinised before the cheque could have been authorised for payment. **Opportunity:** She had the opportunity and used because she was 'trusted' by the government.
How she was caught	This fraud scheme was actually uncovered—strictly by accident, as a result of a credit union employee calling Head of Finance and asking a question about cheques being deposited in a personal checking account. Shortly afterward, it was confirmed that the account in question belonged to one of that county agency's employees. At this point, government auditors were called in and an investigative audit was launched.
Lessons learned	There should be segregation of roles and duties. This would discourage the employees' ideology of 'work-alone' that allows fraudulent activities. No employee should be in a position to write company cheques or make payments without second party confirmation that such payments are valid. Unqualified trust causes an overwhelming number of owners and managers to fail in their jobs because they naively assume that their operation is immune from internal fraud. After all, the managers might argue that they have loyal, long-term and highly trusted employees or volunteers handling their highest-risk financial activities. A few of the managers may understand that whenever trust is incorrectly bestowed, problems are likely to follow.

Table 38: Case #4 Personal Identity Theft Related Crimes: Account Withdrawal

6.3 Analysis of Cases: RetailGroup, Xtail, Ytail, and Ztail

Although data analysis of a semi-structured interview case of this nature normally starts after the data have been collected, the researcher started the data analysis during the data collection. This strategy allowed the researcher to ease the difficult task of dealing with huge amount of recorded data and field notes. Having adhered to Yin (1994) suggestion that analysing case study data is one of the most difficult tasks in developing a qualitative research, the researcher used the approach of content analysis. This approach was used because it allowed the research to make replicable and valid inferences from data to their context (Elo and Kyngas, 2007). This approach enabled the researcher to derive knowledge, new insights and a representation of facts and practical guide to action (Krippendorff, 1980). Since the *RetailGroup*, *Xtail*, *Ytail*, and *Ztail* case studies were designed to examine the application of a role-based framework, the choice of content analysis allowed the researcher to test theoretical issues to enhance the understanding of this research problem (Yin, 2003).

In addition, Berg (1998) suggests that content analysis can be used to examine written documents and transcripts of interviews and to compress many words into fewer content categories based on explicit rules of coding. Hsieh and Shannon (2005) agree with Berg (1998) and suggest three approaches to content analysis: conventional, directed and summative. The researcher applied conventional content analysis where the coding categories are derived directly from the text data built on the following procedures;

i. The recorded voice data from the *RetailGroup* was transcribed verbatim and field notes from the *Xtail*, *Ytail*, and *Ztail* documented were stored as computer files;

ii. Both computer aided software (Nvivo 10) and manual coding were used to ease analysis. In particular, the choice of both computerised and manual coding for *RetailGroup* was used to provide more reliable, comparative and complementary research results (Gibbs, 2002; Bazeley, 2007). In addition, the computerised coding was chosen because of the time-consuming nature of manual coding (Carley, 1990). Similarly, manual coding was used in *Xtail*, *Ytail* and *Ztail*. Though it was time consuming but due to the nature of the convergent interview in these participant observation cases, manual coding was deemed most suitable (Lewis and Silver, 2007).

iii. The coded texts in the form of words and phrases were examined for the co-occurrence of the concepts and how they relate to each other. This is based on the suggestion by Smith and Humphreys (2006) that identified conceptual and relational analyses as the two major categories of content analysis.

iv. The model of themes and matrix in a form of a table of the responses was developed. The matrix table as suggested by Huberman and Miles (1985) enabled the researcher to depict the main relationship between research questions under defined categories and themes.

v. The deductive and inductive codes were derived. This is based on the Benard (2000) suggestion that code-based content analysis enables the researcher to conduct deductive coding via generation of themes from the literature and assigning relevant concept from a set of data. Similarly, inductive coding allows the researcher to generate themes from the data itself which underpins the grounded theory approach (Richards, 2010).

This procedural approach to the content analysis adopted allowed the researcher to provide a comprehensive framework to commence the data analysis (Yin, 2003). It also helped the researcher to connect the finding and results of this research to the existing body of knowledge identified in the literature review of the chapter 2 above (Saunders *et al*., 2007).

6.3.1 Results and Findings from Retail Group

In this case, coding approach helped the research to focus on phrases that are indicative of the research questions and objectives. Based on the procedure of content analysis discussed above in section 6.3, the coding scheme was re-examined by critical analysis of the coding results to validate the reliability. For instance, the delay that arose in trying to incorporate the enforcement agent into the investigation of IIDTRC incident was coded 'Lack of Management Support'. Such issues are broadly categorised under 'Factors those affect IIDTRC Prevention'. Similarly, 'Unclear roles and responsibilities' was coded under the 'Management roles challenges' subcategory. The research eliminated each of the subcategories that did not result in an inefficiency of the crime prevention management or loopholes in the internal IT security tools. For instance, on one of the crimes incidents reported, the local distribution driver (colluded with suspected call centre staff) was a suspect.

However, since this incident involved local distribution employee under logistics management, this incident (though indirectly related) was considered in this analysis. The research questions outline in the section *5.3.2.6 of chapter 5 above were* analysed by categorising the responses of each of the participants under themes in relation the research findings. Similarly, this pattern of analysis was used for all findings from *RetailGroup* in relation to the phrases in subcategories that indicated the IIDTRC a prevention issues. Since each of the subcategories featured multiple issues from respective respondent, they represented IIDTRC prevention issues which may have witnessed in *RetailGroup* but were not specific to any single IIDTRC incidence. Hence, using the process of systematic coding across participants in various management positions, and by comparing their anecdotes and generated codes, the research was able to arrive following findings;

i. Nature of internal identity theft related crimes (IIDTRC) in *RetailGroup*: This includes the causes, the Impact, the perpetration methods and prevention strategies in *RetailGroup*:

ii. Roles of *RetailGroup* management in prevention of IIDTRC: This covers collaboration/support across management in implementing IIDTRC prevention strategies;

iii. Challenges of implementing IIDTRC prevention in *RetailGroup*: This includes challenges that affect management as individual/team in preventing IIDTRC.

6.3.1.1 Nature of IIDTRC in the RetailGroup

The 12 management interviewed on the questions of the nature of IIDTRC in Retail Group provide a clear definition of IIDTRC in the context of *RetailGroup*. In particular, the Group Data Compliance manager referred to the UK Fraud Bill of 2006 and UK Home Office definition.
In her statement,

> "*Identity theft occurs 'when sufficient information about an identity is obtained to facilitate identity crimes or fraud, irrespective of whether in the case of a person, company, organisation or an entity…And this could lead to frauds of using a false identity or someone else's details for unlawful activity. …it could be also when someone avoids falsely claiming that the criminal was the victim of identity fraud….; these frauds come in a variety of ways and for various motive*."

She went on to say that *RetailGroup* have has cases that involved using a false identity or someone's personal identifiable information (PII) (e.g. name, address, date of birth) for financial/commercial gain. The perpetrators use the PII to buy goods or secure services (e.g. opening bank account for money withdrawals) or for credit cards, loan applications, contract services and sorts.

Internal Identity Theft Related Crimes Perpetration in *RetailGroup*

In the follow-up questions, the Group Data Compliance manager were asked to explain what she meant by '*these frauds'* – the variety of ways IIDTRC are committed. She stated that the main techniques for stealing the customers data were: copying the customers details from the systems, diversion of the ordered products, selling of the data to the black market; organised crime - collusion, collaboration and infiltration, computer means, hacking, research of customers ' identity, buying customers data from employees with unrestricted access.

In one of the scenario described by the Regional Loss Prevention manager, he narrated IIDTRC incident where an employee paid an estate management agent to lease him a house for the purpose of collection of the redirected ordered goods from *RetailGroup*.

Most of the participants noted the social engineering which involved an employee revealing the customers data details to an external criminal that called the *RetailGroup* pretending to be the real customer. They also cited the cases when some external criminals would call into the call centres' departments pretending to be from *RetailGroup* IT department, and then would ask for the customers' data or password retrieval. In her own contribution to the question of the methods of carrying out IIDTRC in *RetailGroup*, Head of Human Resources noted that her company is always targeted because of the nature of their business operation. In her statement,

"RetailGroup deals with human beings and knowledge-based design computer systems; these systems are not automated….there is always a need for identification and cross-verification, and in these processes, the customers data could be made vulnerable to the criminal or dishonest employees…"

She noted that the company is working hard to reduce or minimise these incidents, especially in this age where *RetailGroup* business operation is trending speedily on digital means.

Impact of Internal Identity Theft Related Crimes in *RetailGroup*

A few of the participants responded to the question of the nature of IIDTRC in *RetailGroup* in relation to the impact of IIDTRC. In particular, the Regional Loss Prevention manager noted that *RetailGroup* Loss Prevention team handled hundreds of the cases every year, but they could not save all the incidents reports. Some of the incidents reports come from the call centres and from the employees handling the financial details of the customers. In some cases, the Regional Loss Prevention manager noted that *RetailGroup* employees may not be comfortable to report some of their work colleagues engaged in IIDTRC. In his statement,

> '*there have been cases when some of RetailGroup brand's companies came on the national newspapers and national television stations, ... and sort like that, on the issues related to identity theft involved with our employees…such could be a big blow to our businesses and marketing sector….*'

Collectively, the participants have noted similar impact of IIDTRC to *RetailGroup*: business loss, loss of customers trust, job loss, data security challenges, huge budget allocation goes into job recruitment, training, data security, software security, investigation costs, litigation cost , information security auditing; big challenge to the directors and management, damage to business name, and no records of approximated companies' loss.

Methods of Internal Identity Theft Related Crimes Prevention in *RetailGroup*

On the further questions in relation to how *RetailGroup* prevent IIDTRC in their business operation, majority of the participants mentioned these practices (though with various opinions) which include:

- Employees training on data protection,
- Secured customers' data identification,
- *RetailGroup* computer use policy,
- Effective implementation of it security tools: anti-virus and firewalls, intrusion detection and penetration test,
- Restriction on the use of pen and paper and mobile phones,

Employees Training on data protection: In particular the Training Manager and the Head of Human Resources noted employees' training as one of their key IIDTRC prevention strategies. When the Head of Human Resources was asked to explain more on how Employees Training in the *RetailGroup* has contributed to the prevention of IIDTRC, she stated that

> '*RetailGroup design their training resources to match the demand of the various operational departments…, but we focus majorly on the call centres and mail ordering, and less often on the IT security guys…we would always emphasised on Data Protection Act and the consequences…'*

She also noted that every newly employed are mandated to do the online training on Data Protection Act. The employees are also mandated to pass the assessment that follows the training, she added. When asked if there is training evaluation tools designed for the Retail employees in relation to IIDTRC prevention, the Head of Human Resources noted that there is none at the moment. In addition, none of the participants noted any structure for further training either on internal data security or IIDTRC prevention awareness. From her explanation, there was no follow up on how the training was perceived by the employees to enable the *RetailGroup* evaluate the impact of Employees Training in the prevention of IIDTRC.

***RetailGroup* computer use policy:** On the list of top-coded strategy for prevention of IIDTRC in *RetailGroup* is computer policy. All the participants but one made reference how vital this strategy is to *RetailGroup*. They noted that as an employee of *RetailGroup*, you must: have a unique employee login, be ready to change access password regularly, not allowed to download application from internet to the company's systems, not have access to internet or social networking sites, not use either pen and paper or mobile phone while working (except the top managers) and employees must be compliance with password policy. In his response to the question related to the policy issues as a strategy of prevention of IIDTRC, the Compliance team manager said that,

> "*… no employee in RetailGroup from the top management to the shop-floor employee is allowed to access another employee login detail or access code to department terminals, no matter the situation….as you could as well know that exchange of login access would lead to complexity if there were leakage or such IIDTRC incidents as you refer it…besides….,*

…if these principles of our policy is not enforced effectively, all of us would develop the attitude of not taken the policy serious, I mean the 'easy going' culture of business operation…"

This statement shows that the Compliance team manager of *RetailGroup* attached much importance to their policy implementation. But in response one of the participants, the Technical Security Specialist disagreed with the Compliance team manager, and said that '*occasionally, if an employee is locked out, and there is need for the access to the system or department, we could arrange for their access…'* If the *RetailGroup* security has an exception for some managers, this might lead to some leakages involving the top management. These responses indicated that there were existing loose attitudes in relation to the *RetailGroup* security access and policy implementation, which may hamper any IIDTRC incident and render such incident very difficult to trace without complexity. And this suggests there is some preferential treatment approach in security issues in *RetailGroup*.

Secure customers' data identification: A few of the participants noted the secure customers' data identification as one of the *RetailGroup*'s strategy in the prevention of IIDTRC. They emphasised that this is one of the vital strategies in *RetailGroup*, which involves the use of intelligence system in the call centres department to confirm customers' identity. This is a knowledge-based system of using identifications; either of name, address, account number, date of birth or combination of any of any of the identity attributes. The Head of Security Operations in his response to this strategy stated that;

"*RetailGroup has designed this system in such a way that identification processes and questions involve some element of complexity to deter the criminal within or from outside our company to access customers' sensitive data….but the problem with system is that our employees a times failed to implement the processes effectively, they allowed or forgot…perhaps unintentionally allows customers or suspects to access their data without asking the security questions…"*

This response suggests that there were occasions knowledge-based systems have failed in *RetailGroup*. It also suggests that Retail Group relied heavily on this system and that *RetailGroup* is aware of the need for effectiveness of the system. Yet there is no sign in *RetailGroup* to support and improve the efficiency of the employees on how to make use of the system. The implication of this issue is that if the system fails and the company relied upon the system for security of the customers' data, there would high risk of IIDTRC incident on such occasion.

In summary, the model below describes the nature of internal identity theft related crimes in *RetailGroup*.

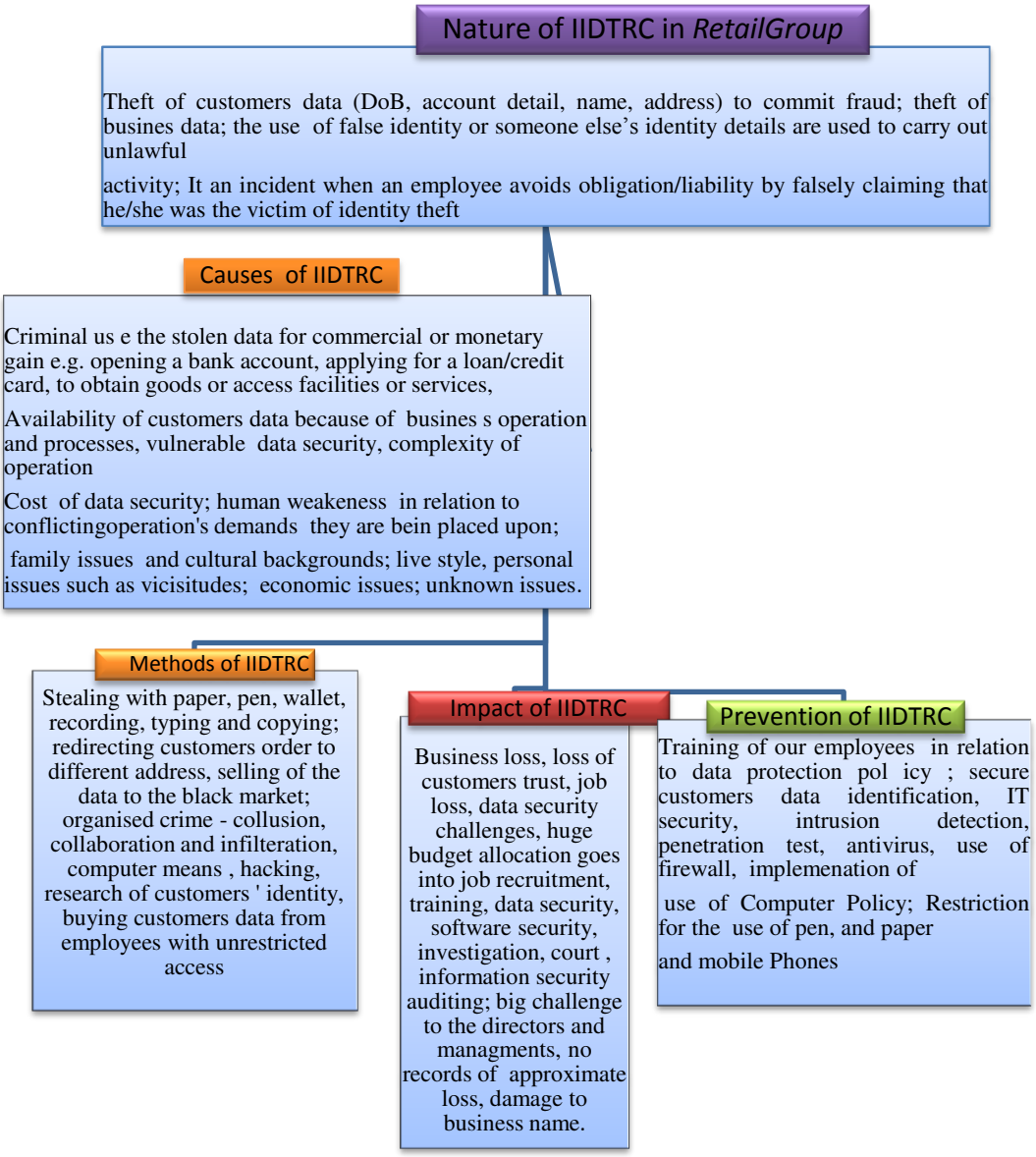


Figure 14: Nature of Internal Identity Theft Related Crimes in *RetailGroup*

6.3.1.2 Roles of RetailGroup Management in Prevention of IIDTRC

All the participants agreed that sharing their roles and responsibilities in relation to IIDTRC prevention is vital to the success of *RetailGroup* in IIDTRC prevention. In some cases, they extended to some supporting roles that have contributed to their performance enhancement in *RetailGroup*.

As the summary of the roles collaboration, the table 44 below shows the model matrix mapping the participant roles in IIDTRC prevention team roles. The participant's management position relate to various roles which include: Security Support (SecSup), IIDTRC Incident Investigation (IIDTInv), Data Compliance (DCMgt), IIDTRC Prevention(IDTPrv), Security Operation(SecOp), Technical Security(TecSec), Software Engineering(SofEng), and Human Resources (HR) denoted the team roles.

Roles / **Mgt. Position**	**SecSup**	**IIDTInv**	**DCMgt**	**IDTPrv**	**SecOp**	**TecSec**	**SofEng**	**HR**
Head of security support	×	×		×	×		×	
Head of crimes investigation		×		×				
Group Data Compliance manager			×					
Head of Crimes prevention		×		×				
Head of Security of Operations	×				×	×		
Technical security specialists	×	×			×	×	×	
Training Manager								×
Software Engineer	×						×	
Compliance team manager			×			×		
Technical Security Specialist	×				×	×		
Regional Loss Prevention manager		×		×				
Head of Human Resources		×						×

Table 39: Matrix of Management Positions with Roles

The table coding analysis indicated that these roles do not necessarily related to individual participant's management position on a one-to-one basis; showing that one participant might have covered two or more roles, or a role could have been split between two or more participants.

In the statement by the Regional Loss Prevention manager,

> "*on some of the IIDTRC cases, we have to involve the crime investigation team (*Head of security support*)…once the incident have been escalated, it starts with the* Head of security support *who would do the internal incident investigation with his team and send the report back to me for further action to be taken…"*

And when the Regional Loss Prevention manager was asked further questions on how timely and efficient is this sharing of responsibility, he stated,

> "*…well it depends the impact of the case and the complexity and how many employees are involved…, I cannot really give the approximate time it takes because some of these cases take longer than expected…, There might cases the involve criminals from different RetailGroup branches…These issues take lots of resources from the company…"*

This statement suggests that issues such as the seriousness of the IIDTRC incident, geographical constraints and staff availability can have an impact on the setting up of the ideal management team for IIDTRC prevention. This statement suggests the need for the management roles in relation to IIDTRC prevention to be clearly considered and assigned appropriately with respect to the nature of IIDTRC – place, who, how and when the crimes were committed. In particular, the management involved need to be fully aware of their responsibilities.

However, from the matrix table above, it shows there is a collaborative role sharing among the management, but some of the vital roles are being neglected. For instance, the training manager position collaborated with none of the participants but Head of Human Resources. This indicated the total negligence of the role of IIDTRC prevention awareness in *RetailGroup*. Another participant role that was neglect by the *RetailGroup* is Data compliance management. This shows that less attention was given to the contribution of the data compliance in the IIDTRC prevention working team. This consequence of this negligence would lead to an overly non-compliance culture of the majority of the internal data security of the Retail group, of which the potential cost is increasing the risk associated with data leakages and IIDTRC incidents.

6.3.1.3 Challenges of Implementing IIDTRC Prevention in RetailGroup

In response to the question of the major challenges issues faced by *RetailGroup*'s information systems management in the prevention of IIDTRC, the participants noted that the challenges are not limited to individual managers. They recognised that IIDTRC prevention challenges in *RetailGroup* also affect their collaborative management roles. The analysis below indicates the key issues that affect *RetailGroup* management performance goals. The participants' views are categorised as: Management as an Individual Role and Management as Team Role.

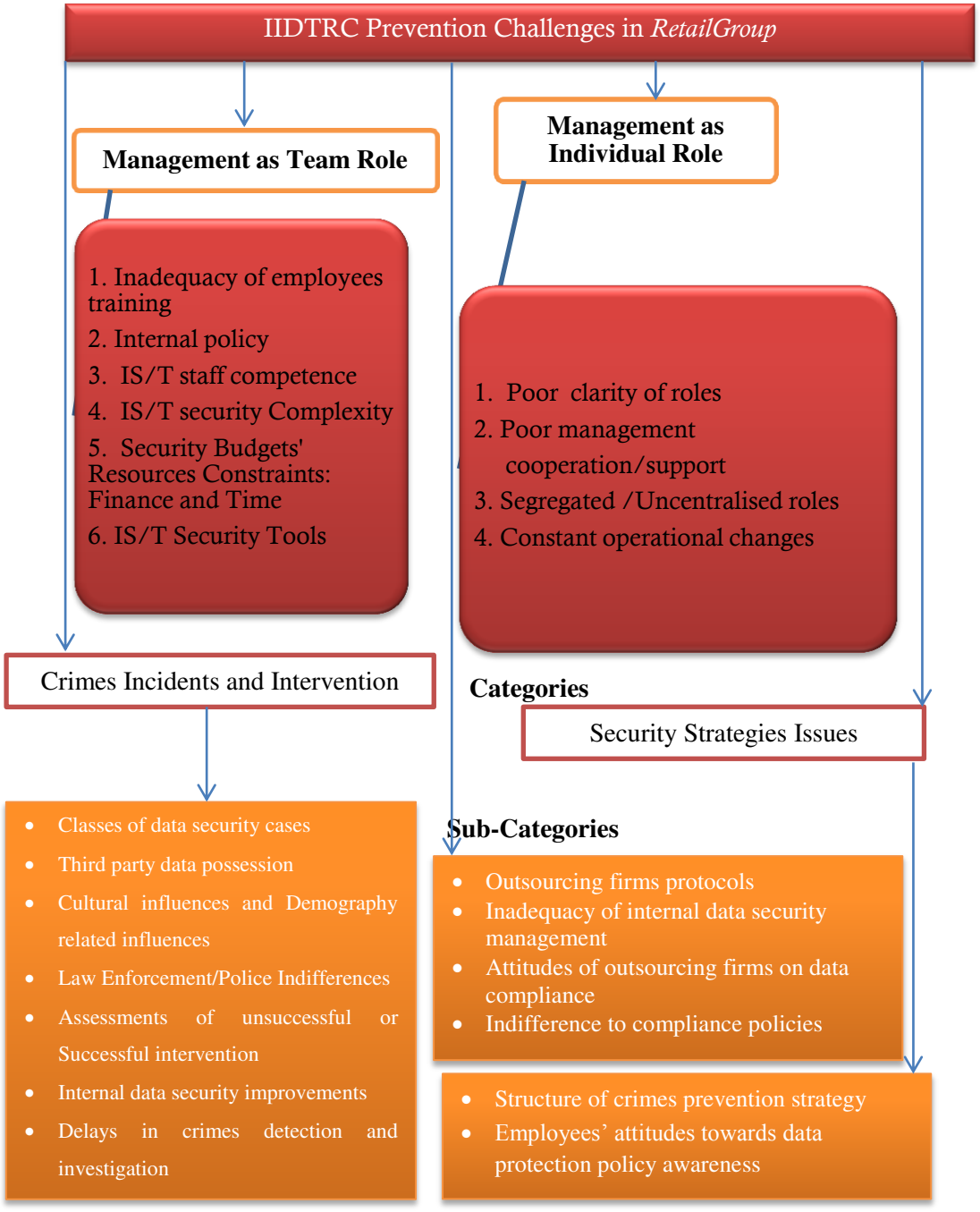


Figure 15: Internal Identity Theft Related Crimes Prevention Challenges

Figure 15 below shows the model of the 10 factors that were consistently identified with the 12 participants, arranged in the order shown in the coded description. Unclear responsibilities, lack of employees/end-user awareness training and lack of management cooperation/support top the coded factors in both categories.

Challenges of management in their individual roles of preventing IIDTRC

Clarity of Roles: Some the participants were not clear with the commitment that is required of them in the prevention of IIDTRC. Although, a few participants explained how they pay attention in identifying the vulnerability by classifying the internal data security cases. Without clear responsibility, as indicated in *RetailGroup*, the overall IIDTRC prevention and internal data security would be handicapped. Most of the managers narrated stories of their experiences but were not reflective of what their key roles and responsibilities are in relation to IIDTRC prevention. This shows that participants from *RetailGroup* were busy with their routine of IIDTRC escalation process; detection, investigation, etc. They are more committed to meet their targets of completing investigation cases than reflecting on the requirement of their job roles. In *RetailGroup* business environment, it would not be a surprise that strategic IIDTRC prevention processes are put to a lower priority.

Management Cooperation/Support: The Head of crimes investigation made mentioned of the difficulty his team faces in trying to build effective working relationship with the management of the local law enforcement agency. He noted that this issue often led to delays in investigation of crimes:

> "*When there is the change of the head of local area police, all the long built relationship and working team would breakdown…, to build up a relationship with the new administration is not easy! Sometimes it is not easy to find the police officer that would play the role of effective investigation of IIDTRC…it is always problem…it is, yes it is…this always lead to delays of investigation and prosecutions……*"
>
> This statement suggests that establishing a lasting support with the law enforcement agencies is a major challenge to *RetailGroup* managers in their bid to prevent IIDTRC. This challenge is can be a major factor that may have led to the cases of protracted IIDTRC investigation process in the *RetailGroup*. The longer the investigation took, the more damage the perpetrators would do with the stolen data/information.

Segregation of Management Roles: There was indication that participants have varying perception in relation to IIDTRC prevention in *RetailGroup*. It was observed that different management roles have different perception about data security and regulations. The shop floor managers see internal data security regulations and IIDTRC prevention as the business of the top management alone. From the response of the Software Engineer, when asked to describe his cooperation and working relationship with the management, he said;

> *"I would always continue with my major job roles, which is basically designing of 'RetailGroup' secured systems applications, when the need for computer crimes issue comes up, the management handles those…"*

This statement suggests and confirms the perception of segregation of duties that many *RetailGroup* managers stick to their job roles without contributing to internal data security and IIDTRC prevention.

Operational changes: Some of the participants are concerned about the operational changes (such as reduction in IT security budgets and shuffling of staff management positions) and the impacts of the IIDTRC incidents in the *RetailGroup*. A few of these participants perceived that the rate of a trend is beyond the capability of *RetailGroup* to match. For this reason, they utilize the resources they have at their disposal to implement the latest security tool for prevention of the IIDTRC. Other key issues that pose challenges in the prevention of IIDTRC in the *RetailGroup* include the budget constraints, the employees' expertise, and pace of the evolving digital security technologies. In responding to the question related to challenges of implementing up-to-date security tools, the Head of security support said

> "*Well, these security tools are not cheap, and we are talking about RetailGroup of many branches spread across UK…., besides, the security companies never stop designing new product…em, we cannot go beyond the company's budget...*"

This statement suggests the impact the operational changes have as one of the major challenges of *RetailGroup* management.

Challenges of management in their team roles of preventing IIDTRC

Lack of Employees/End-user Awareness Training: There were some participant perceptions that effort by the management toward training of the employees is established with independent capability.

It was either carried out by the human resources or never gets done. The attempts to educate all the employees have not yielded expected result. They noted that the setbacks on the employees' awareness training on prevention of IIDTRC may be associated with the cost of human resource development. Besides, most of the available data security policies are not clear enough to the level of understanding of the shop floor employees. *RetailGroup* may have mandatory e-learning (data protection policy and regulations) that was designed to meet the educational requirements and levels of all management and employees, but is this achievable in *RetailGroup*? In response to this question the Head of Human Resources stated:

> *"We have to ensure that our employees are trained and are updated on data protection policy. My management team in this organisation takes these steps as our responsibility. We have designed a comprehensive training programme for the employees across security management. I spent weeks to design the structure of the training package myself. I want everyone, irrespective of the level, to know the consequences indulging in any data security violations… there should not be any excuse to commit internal frauds!"*

The Head of crimes Investigation corresponded and remarked:

> "*All our employees are required to go through this test and they have to pass them. We have their respective profile, we will always check. If any of them failed to attend the e-learning test, we have to find out why and encourage them to do it. It is not just for the security of the customers date, my team, or the organisation…it is for the security of their job!*"

In agreement to these anecdotes, the Software Engineer noted:

> "*I have just attended one week training to update myself not only on the latest security resources; the training availed me the opportunity to go through the data security policy and sorts like…"*

These affirmations indicated there was training on data protection, done online by the employees, to ensure that the employee would abide by the data security policies and stipulations, but not particularly on IIDTRC preventions. In addition, these statements suggest that *RetailGroup* depends only on their Human Resource Management for IIDTRC awareness training.

Lack of Clarity of Data Protection Policy: Without the well-defined policy in *RetailGroup*, it may be difficult to outsource to other companies on the issues of IIDTRC prevention. Some of the participants noted that a majority of the third party companies rarely '*buy in'* or adhere to the stipulated data security agreement. They handle with data internal data security with laxity. In most cases, they do not put in place the security checks and measures to avoid any accidental data leakages or theft that might arise during transactions. The Compliance team manager described the practices of the outsourcing companies thus:

> "*When 'RetailGroup' outsources some of these firms to manage our customer data, they rarely comply with the stipulated data compliance regulation! They would only tick the papers to prove that all the data security checks are up to date, but during my visit for data security auditing, I would find out that there were some security laxities. All those protocols are just shown on the papers…., It is all about ticking paper. They don't care about our data security, their clients... they never see this as their responsibility – which is their major role as our agency!"*

In agreement with the Compliance team manager, the Head of Crimes prevention noted that though *RetailGroup* have a contractual policy binding the outsourcing firms, the firms still treat IIDTRC prevention policy as 'their business' (*RetailGroup* business). To control these pervasive attitudes of the outsourcing companies, the data compliance management has resorted to the strategy of coercion and thorough data security auditing. If these strategies failed *RetailGroup* would revoke their business contract with the outsourcing firms. The *RetailGroup*'s Data Compliance Manager described her recent experience:

> "*We have just revoked a contract with one of the outsourcing companies because of their laxity in abiding by our stipulated data security measures…We requested for the print out of all network security test updates of which they provided. We found out that there some of the test that was not successful, we then asked then to update that and resend the results….but they failed to implement our request. We have no other option than to revoke the contract!"*

These statements suggest that *RetailGroup* might not have adequate staff expertise and resources for prevention of IIDTRC since they were consistently referring to the outsourcing firms as the key provider of their security support,

Lack of Trained IS/T Staff: The instances where the respondents consistently referring to the partners and outsourcing agents suggest that *RetailGroup* could not provide the necessary staff expertise and resources in the prevention of IIDTRC. The practice of outsourcing or hiring external agent in *RetailGroup* may have strained the management effort in establishing the effective cooperation and sharing of responsibilities in relation to IIDTRC prevention. This issue extends to other factors in relation to lack effective communication and role sharing with other complementary management such as law enforcement agencies. As noted above, the lax attitudes of the outsourcing and law enforcement management in cooperating with *RetailGroup* is a major setback. The Group Data Compliance manager in her response said that:

> "*Most of these agencies' management do not have good knowledge of data security expertise in carrying out their responsibilities in the prevention of the IIDTRC as compared to what is obtainable in this organisation….*"

She added this issue often delays investigation protocols because of roles clarifications issues such as '*who does what and where do we go first'* in handling internal data security breaches.

IIDTRC and IS/T Security Complexity: There was perception from the participants that complexities of IIDTRC issues such as the 'seriousness' of the crime, culture, and outcome of a crime incident, interfered with their security strategies.

On the issue of incident assessment and interventions, the management is aware of the importance of the aftermath assessment of intervention processes of typical IIDTRC incidents. They also believe that it contributes to the improvement of the data security strategies. However, they still struggle with issues related to crimes incidents analysis and documentation. The Head of Security of Operations noted regrettably:

> "*We have not really got documented reports of all the procedures taken during the investigation…, these kinds of crimes happen over and over again. Whenever we handed the criminal case and handed the suspected over the prosecution team, that closed the case…but we do not document and analysed the incidents of closed crimes cases….You see these could cost a lot of money, take lots of times and expertise. Besides we need to hire professionals to do that…"*

This statement suggests that some of the IIDTRC preventions or interventions may have failed in the *RetailGroup* because of the management perceptions in handling their complexities.

Poor IS/T Security Tools: The participants noted that there are cases where security loopholes were discovered within the IT platform and were neglected because management viewed it as not being cost effective to upgrade or because it does not really constitute high risk. The IIDTRC incidents are rated from high-risk issues to low risk issues. Perception like this affects the roles of the data security expert in the design of the data security tools like encryptions for the security of such data. In addition to the respective management as an individual and team-oriented challenges identified in the analyses above, there are other issues that affect both categories of roles. Other notable issues perceived by the participants include;

Poor Internal data security control and strategy: - Among the top IT security and crime prevention team, internal data security was their prime responsibility but their attitudes towards internal data security control were perceived to be in a poor state. Though, these management received the some level of support from other complimentary management such as human resources, software engineering and network/web administrators, there is no collaborative strategy within *RetailGroup*. This issue has led these complimentary management team to place a lot of emphasis on abiding by the data security policies of *RetailGroup* but neglecting the key aspect of IT security which internal security control.

Management attitudes towards IIDTRC interventions outcomes: The management were aware of the importance of the aftermath assessment of intervention processes of typical IIDTRC incidents; and its contribution to the improvement of the data security strategies. Though the top management from both the IT security and crime prevention team meet as frequent as possible to reassess their performance in the prevention of crimes, they still struggle with issues related to crimes incidents analysis and documentation.

It was observed that some of the crimes prevention or intervention failed because of inadequate resources – money and security experts. They participants cited some cases where some security loopholes were discovered within the IT platform; these loopholes were neglected because the organisation viewed it not being cost effective to upgrade or because it does not really constitute high risk. The IIDTRC incidents are rated from high-risk issues to low risk issues. If the crimes involve theft or loss of with certain attributes of personally identifiable data, then it is then classified as high/low-risk crime.

Cultural orientation of the management: Drawing from the interviews of the *RetailGroup*'s information systems (IS) security and crimes prevention management, cultural orientation has been identified as one of the major challenges of preventing IIDTRC in the retail companies. This finding from the *RetailGroup* suggests that the cultural orientation of the management affects their information security roles in preventing internal identity theft related crimes (IIDTRC). Tsai (2001) explains that cultural orientation is the degree to which employees are inclined and a way of actively engaged in the norms, practices and traditions of a specific organisational culture.

Cameron and Quinn (1999) throws more light on the issues of culture within the organisation by defining organisational culture as a set of shared assumptions, beliefs, practices and values that direct and shape members behaviour and attitudes. These definitions of aspects of culture within organisational setting provided an insight to the finding of this research where one of the major challenges in preventing IIDTRC is caused by the cultural influence of IS security managers. Based on this finding, it is worth concluding that the cultural orientation of IS security management could be the root of other challenging issues.

Other key challenges of preventing IIDTRC that embedded in the management cultural orientation of the *RetailGroup* are: management believes that IS security is a complex issue; constraints in getting adequate budget for IT security; lack of clarity of roles and responsibilities, internal security policies and strategies and perceived IIDTRC incidents.

There exist a belief by IS security and crime prevention management of the *RetailGroup* that prevention of IIDTRC is a complex security issue. The crime prevention managers are inclined to treat information security regarding the prevention of IIDTRC as troublesome and often depend on software security. Consequently, the management resists new policies that might be strategic in preventing IIDTRC. This belief reflects reason for Chia *et al.,* (2003) argument that without change in cultural of orientation of IS security managers, the enforcement of new policies regarding computer related crimes prevention might not be optimal.

In the same vein, the cultural orientation of the management regarding the prevention of IIDTRC constitutes to constraints in getting adequate budget for IT security in the *RetailGroup*. For example, the management of the *RetailGroup* are inclined to treat spending related to IT security as a financial burden to their company and are often reluctant to support IIDTRC prevention initiatives. Instead of investing to improve

their IIDTRC prevention strategies, the management relies on their managerial experience and contingency plans. This is evidenced by the comment of the *RetailGroup*'s Head of Security Operations (HoSO) regarding his belief in the importance of investing in IIDTRC incidents analysis and documentation. The *HoSO* stated that;

> "*We have not really got documented reports of all the procedures taken during the investigation…, these kinds of crimes happen over and over again. Whenever we handled the criminal case and handed the suspected over to the prosecution team, that closed the case…but we do not document and analysed the incidents of closed crimes cases….You see these could cost a lot of money, take lots of times and expertise. Besides we need to hire professionals to do that…"*

This statement suggests that some of the IIDTRC preventions may have failed in the *RetailGroup* because of the management cultural orientation that there is no need to invest in innovative IT security initiatives if there is no apparent security threat. This evidence corresponds to Straub's (1986) argument that some business organisations neglect the strategic IS security practices because they have not had any major loss to computer crimes related threats. In addition, this evidence support the findings by the PriceWaterCoopers' (PWC) (2014) Survey that more than 56 per cent of business organisations did not carry out any security checks of there IS security infrastructure, instead they only rely on contingency plans.

In some cases, PWC (2014) further added, online retail companies apparently consider themselves '*not rich enough*' to bear the cost of IS security. Other companies often argue that the cost of IT security investment outweighs the benefits. However, the *HoSO* of the *RetailGroup* defended the position of top management for not investing in security tools recommended (for preventing IIDTRC) by their IT security managers. The *HoSO* argued that in most cases there is no clear information that suggests that there is a substantial impact of existing IT security invested in preventing IIDTRC. This evidence is drawn from *HoSO's* statement that;

> *"RetailGroup operates on different security strategies in terms of the resources: soft and hard, and the degree of the access the companies grant to management over IS security investment. Management are supposed to report/publish the impact of their security strategies in preventing IIDTRC but when this reporting is not done it would be hard to evaluate the benefits of IS security investment and strategies".*

In this manager's view, the management should work collaboratively with the top management by updating them with information on how the implemented security tools have impacted on the IIDTRC prevention. This view suggests that if *RetailGroup* has cultural orientation for providing a collaborative support and opportunity from top management (on IS security strategies regarding prevention of IIDTRC) with clearer roles, *RetailGroup* would be less prone to IIDTRC. This is because decision-making on crimes prevention would be more distributed in the *RetailGroup* although the top management retains oversight and accountability for IS security/compliance investment probity.

Other effects of the cultural orientation of management on IIDTRC prevention

In addition, there was evidence by the *RetailGroup* that the cultural orientation of the security management can weaken the security strategies in preventing IIDTRC. The *RetailGroup* was restricted to their internal data security strategies and policies. The implementation of their security policies was directed by internal *RetailGroup*'s requirement but not from the belief in the importance of security practices. In this case, the *RetailGroup* management considers innovative information security strategies as inconvenience. This finding corresponds to the Maynard and Ruighaver's (2006) conclusion that a number of business organisations are forced to conform to existing internal data security compliance and security roles. This conclusion is evidenced by the comment of the *RetailGroup*'s data compliance manager;

> "*We are extraordinarily well-organised security management team, and every member of our management team work for what it's worth in their roles in preventing IIDTRC. People have been very hard working, but we're moving beyond the point where grace will win the day if managers begin to switch their roles".*

This comment shows that *RetailGroup* managers are explicitly empowered to intervene and make independent decisions in order to address challenging data security issues, but this can militate against them following if they consider alternatives to their existing roles and responsibilities. Similarly, a comment from the Software Engineer from the *RetailGroup* reaffirms that the issue of cultural orientation has impacts on the roles and responsibilities of security management and security managers are more concerned about his or her peculiar roles.

This is evidenced by the comment from of the Software Engineer, when asked to describe his cooperation and working relationship with the other management team, the Software Engineer said;

> *"I would always continue with my major job roles, which is basically designing of 'RetailGroup' secured systems applications, when the need for computer crimes issue comes up, the management handles those…"*

This statement corresponds to perceptions of the *RetailGroup*'s Data Compliance manager that the cultural orientation of the management. These perceptions revealed the common belief in the *RetailGroup* that each manager has to stick to their job roles with little or no contribution to the collaborative effort regarding internal data security and IIDTRC prevention. Only the top management are involved in designing and implementing security strategies in preventing IIDTRC. The shop floor managers see internal data security regulations and IIDTRC prevention as the business of the top management alone.

However, Popa and Doinea (2007) argue that issue of cultural orientation where only the top managers are concerned with the issues of IIDTRC incident might linked to perception of top managers regarding the sensitive and complex nature of IIDTRC.

Popa and Doinea (2007) suggest that some businesses managers often do not trust the capabilities of the shop floor security and data compliance management. In some cases, companies perceive data security issues regarding IIDTRC prevention as a complex security practice that requires the expertise of top data security management. In agreement to Popa and Doinea (2007), Koh *et al.,* (2005) suggests that because of nature of IS security in business organisation only small group of management is involved in implementing IS security strategies against IIDTRC and this could pose a major challenge in the business organisations. Hence, the issue of addressing the increasing workloads of preventing IIDTRC with a few management teams requires a strategic balance between company owners and the management.

Furthermore, some *RetailGroup* security management believes that amount of attention that would be given to particular IIDTRC incident would depend on *the nature* and *the class* of the incidents. This issue of IIDTRC incidents' *characteristics* and *classification* was discussed above as it has an influence on the amount of effort the law enforcement agency/police input in IIDTRC investigation.

In the same vein, security management believes that some IIDTRC incidents should be treated with respect to the IIDTRC incident profile - '*who is'* the perpetrator, *'where' the perpetrator comes from* and *what ethnic origin* is the perpetrator. The IS security management is inclined to think that some employees with some cultural features are more prone to perpetrating IIDTRC than others. Because of the cultural influence in the way the IS security management handles IIDTRC incidents, some of the incidents are not given due attention because the suspect is from '*developed*' countries or *ethnic 'majorities'*. The *RetailGroup*'s Head of Crimes Investigation remarked:

> "*Most crimes incidents we have observed are often perpetrated by the employees from the 'minority ethnic groups'...although, sometimes there are bad ones from this country, but their cases are not as 'that bad' compared to that of those from those 'minorities'."*

This statement reveals that the cultural orientation of the IS security and crime prevention management of the *RetailGroup* influences their roles in preventing IIDTRC. This statement suggests that some of the crime prevention managers seemed to believe that employees from the 'developing' or 'less developed' countries are more susceptible to crimes than those from developed countries. Drawing upon this remark, this research explains that security and crime prevention management held a biased view of the employees as a consequence of only coming into contact with non-abiding law abiding employees from minority ethnic background. This finding is in line with the suggestion by Westley (1970) which explains that security officers within the occupational roles of control often experience hostility from the environment with ethnic minority in which they operation causing them to perceive them as environment prone to crimes.

In a similar study, Skolnick (1966) explains that security officers respond to crimes incidents in a way that predict situations and perpetrators which present the greatest risk to the security management. Skolnick (1966) suggests that security officers refers such perpetrators as the *'symbolic assailant'*, which means a profile of individual whose appearance, ethnic background, demeanour represents an indicator of criminal, irrespective of whether the individual actually commits crimes. Having this occupational culture, Cosgrove (2011) argues that the security officers are inclined to be suspicious in identifying abnormal crimes related activities. In doing so, the security officers gather information on innocent individuals which officers may have assumed to be at the risk of offending in a way that satisfies perception of the symbolic assailant.

Previous literature on how the cultural orientation undermines security compliance with rules/regulations

Previous studies (e.g. Westley, 1970; Cain, 1973; Waddington, 1999a; Scerra, 2011) refer this perception as a culture of 'racial and ethnic minorities prejudice' which is common not only in the police occupation but also in the related crimes prevention setting. In particular, Scerra (2011) characterises this issue of cultural orientation of the crime prevention managers in managing IIDTRC as 'investigating stereotypes'; where the crime prevention managers use stereotypes in dealing with their roles, functions and practices. This issue has also been noted by Sanders and Young (2002) that cultural orientation of police work in UK affects the way police label suspects based on their race and subsequent group. The suspects who fall within marginalised groups in society are often vulnerable to prosecution even when they are not guilty (Engel *et al.,* 2002).

However, this research cannot fully provide answers to question of why IS security and crimes prevention managers of *RetailGroup* act the way they do without considering the meaning the managers ascribe to their actions and the retail business environments. IS security and crime prevention management in the *RetailGroup* is moulded as multicultural professionals that comprise of individuals from multi-facet cultural backgrounds. Newburn and Webb (1999) argue that the issue of cultural orientation is synonymous with challenge commonly experienced by security managers in preventing of business or corporate crimes. They suggest that one of the major factors that encourage a cultural perception of management in the prevention of crimes is a high degree of internal solidarity and secrecy within the security management. They further added that any attempt to curb this influence in a business organisation results in cynicism and displeasure. Similarly, Paoline (2003) argues that crimes prevention managers develop cultural oriented attitudes, norms and values in relation to their occupation as means of adapting to demand of their work and also a means to cope with the scrutiny of their organisational environment.

In addition, McConville and Shepherd (1992) had discussed cultural orientation regarding security management as an occupational issue which common in the crimes prevention settings. They argued that what some lower level and shop floor crime prevention managers learn in their occupation is the need to keep their mouth shut about unethical security practices, including those in breach of the security compliance rules, which experienced managers deem necessary in discharging security management roles and responsibilities.

In doing this, Reiner (1992, p.93) argues that the crimes prevention managers at all levels tend to adopt secrecy as *'a protective armour shielding them from public knowledge of 'culturally oriented unethical security' infractions'*. Newburn and Webb (1999) further added that it is not just about secrecy, but organisational or occupational level of bureaucracy, strong bond of loyalty, rated integrity of leadership, solidarity of characteristics work subcultures, moral career stages of the security managers and perception of legitimate opportunities.

Other sociological studies (e.g.Van Maanen, 1974; Manning, 1989) argue that crimes prevention managers form culturally oriented unethical security attitudes, beliefs and values due to the challenging experiences associated with their occupation of crimes prevention. These studies suggest that working in crimes prevention setting with limited cultural training and a remit for reassurance are likely to be overwhelmed by strains associated with the crimes prevention.

Implication of the cultural orientation in the IIDTRC prevention

The implication of these issues linked to the cultural influence could be significant on prevention of corporate crimes such as IIDTRC. The culturally oriented unethical security practices within 'crime prevention management culture' has been identified in several report (e.g Criminal Justice System) and official enquiries as both encouraging and facilitating inefficiency and hampering security strategies and management effort in crimes prevention (Newburn and Webb, 1999). Fitzgerald (2007) points to the causes of these cultural issue to wider crime prevention challenges which include: inadequacy of educational training of the security managers (especially with regard to culturally oriented unethical security training); abuse of management authority, inadequacy of crimes prevention management or poor security management; disregard for honesty and the truth in crimes investigation; contemptuous attitude to criminal justice system by the crimes prevention manager and rejection of criminal justice system application to crimes prevention.

Moreover, Roukis (2006) suggests that lack of emphasis on the intentions of the employees towards ethical security practices could lead to an absence of organisational transparency. Lack of transparent security practices of management could lead to criminal behaviour; especially when there are occupational challenges and work pressure are hard on the security management.

Roukis (2006) further added that in a highly challenging occupational environmental of crimes prevention, a security manager might be tempted to commit IIDTRC such as intellectual property crimes, fraudulent manipulation of company stocks and paying bribe to business contractors. Roukis recommends that it is vital to get rid of ambiguity from business operational environments and to foster cultural oriented managerial and organisational transparency ingrained where defined ethical practices is a corporate priority. In support of Roukis (2006) recommendation, other researchers (e.g. London, 1999; Dion, 2008) suggests that a 'principled leadership' could be the way for security managers to apply clearly defined culturally oriented ethical business values in their occupational life such as fairness, honesty, kindness and mutual respect.

With principled management integrated with moral courage (use of inner principles to do good regardless the personal risks), Sekerka and Bagozzi (2007) suggest, the managers would be able to make security decisions on prevention of IIDTRC 'in the light of what is good' for the cross-functional management team despite personal risks of cultural orientation. Punch (1994) suggests that the impact of cultural orientation influence in crime prevention can be removed by taking authority to make decisions out of the hands of top managers. (Criminal Justice Commission, 1997) recommends that cultural influences can also be reduced by rotating on a regular basis the roles and position of security managers in 'high risk' or sensitive areas.

The finding from the interviews of *RetailGroup* has provided the knowledge on the impact of the cultural orientation of IS security and crimes prevention managers in the roles and practices of IIDTRC prevention. It has unveiled that the cultural orientation of the management has a huge influence on their roles in the prevention of the IIDTRC. Cultural orientation regarding the organisational culture of the retail companies may not be separated from the IS security management. This analysis of the views from *RetailGroup* shows that various interpretations of IS security management are cultural constructs underpinned by core assumptions and values held by members of IS security management in different roles. These values portrayed by the IS management arise from cultural, ethical, organisational and social dimensions. Drawing from this research findings, one could add that issues of cultural orientation of management in an organisation are socially induced. Thus, criminal events and preventions, the issues of IIDTRC as in this research, are connected to fundamental features of the societal culture that hosts the business organisation. For an effective prevention of IIDTRC in the retail companies, this finding from the *RetailGroup* suggests that there is a need for a change in the cultural attitudes.

This is in line with Braithwaithe's (1989) argument that there is a strong need for a 'change' within organisation culture in preventing crimes. Braithwaithe (1989) suggests that the increased emphasis on managerial responsibility embedded in understanding of cultural influence aimed at ensuring compliance is more likely to have long-lasting benefits in preventing corporate or business crimes than other deterrence via the threat of prosecution. Slapper and Tombs (1999) argue that any focus on prevention of corporate business related crimes implies to examine the crimes inwardly in terms of organisational culture. Organisations present moral value which can symbolise specific organisational identities of their management and employees. Based on this argument, Dahler-Larsen (1997) concludes that management and employees have a role and responsibility to play in the way the organisational operations justify their decision and action regarding security and crimes prevention practices.

The knowledge of the impact of cultural orientation of management as a challenge on the prevention of IIDTRC in a particular retail company – the *RetailGroup* would equip IS security managers with a valuable tool for managing the multicultural dimension of the management workforce. This knowledge would also equip the management to develop a strategic cross-functional and socio-cultural skills needed for preventing IIDTRC, investigating IIDTRC incidents and prosecuting IIDTRC perpetrators. This research, in line with the findings from previous studies (e.g. Skolnick, 1966; Manning, 1995), suggests a link between culture and security practices which is a huge challenge to security management. This suggestion calls for greater precision in future studies to unveil the 'contours of the impact of the culture in crimes prevention', especially investigating those aspects of the occupational security cultures undermining compliance with rules/regulations.

Law Enforcement Agency/Police Indifference: Police indifference is one of the major challenges identified in this research, which the security management in the *RetailGroup* remarked that it is affecting their effort in preventing IIDTRC in their company. Many of the managers interviewed noted that there is a perception that the police officers treat some IIDTRC incidents with indifference. This attitude of indifference is rooted in the perception by the police that there are areas within UK where crimes are believed to be more prevalent than others.

For instance, crimes incidents reports from cities such as London, Birmingham, Manchester and Glasgow are given priority by the police response team because the cities are seen as sites of notoriety for crimes. If IIDTRC incidents reported to the police falls outside these cities, then the police would treat the incidents with disregard.

Berki (1986) refers this kind of indifference from formal state security officers as *'malevolent indifferent'*; which can contribute to feeling of insecurity to not only the citizens but also to businesses. Berki (1986, p.11) explains further that indifference is the disregard meted out to citizens with implied feeling and intention that their interests, desires and security should not count at all and should not be treated in the same way as other citizens.

This perception of disregarding crime report from smaller cities or small business sectors is affecting the police collaboration in preventing IIDTRC in the retail companies. In response to the question of 'what is the attitude of the police in assisting the *RetailGroup* in fighting IIDTRC', the Regional Loss Prevention manager stated:

> *"We have very good relationship with the police…, with my twelve years of experience in the law enforcement agencies we direct our efforts to major cities… - London, Manchester, Liverpool, Glasgow and Birmingham and 'crimes' hot spot', in the business environment, the banking sector has been a big target compared to other businesses."*

This issue of indifferences in some cases is a misconception, which often lead to negligence on the part of management efforts in preventing IIDTRC in the online retail (Prenzler, 2009). This misconception may interfere in some ways the law enforcement agency view the crimes in the society which may lead to cases of IIDTRC from the small cities being neglected to the detriment of the businesses in those cities. The incidents of IIDTRC may continue to increase in the online retail companies unless the police changes their attitude of indifference to crimes investigation and give equal attention to every crime irrespective of cities or the sector the crimes were committed, whether they are high profile crime or low profile crime. This research suggests that police are overwhelmed with the perception that since other crimes are rampant in bigger cities so would be the IIDTRC. This suggestion points to the reason the police believe that IIDTRC crime can be tackled like any other crime. And this evidence corresponds to researcher's (e.g. Flanagan, 2008; Rix *et al.,* 2009) suggestions that police rarely cooperate in investigating IIDTRC because these crimes emerge from retail sector which is a small sector compared to banking sector.

In addition, Ashworth (2005) notes that police would rather get themselves involve with high value or violence crimes. Bamfield (2012) agrees with Ashworth (2005) and argues that although retail crimes such as internal identity theft related crime might be important to the police but may not be one of the top priorities central to their crime prevention strategies. The issue of police indifference in cooperating with retail management in combating IIDTRC might leave the management open to potential litigation for unlawful arrest. This might be the case if a suspected IIDTRC perpetrator was arrested without police cooperation and held for somewhat too long.

When the *Head of Crimes Investigation* from *RetailGroup* was asked about the how the *RetailGroup* cope without the police cooperation during the investigation of IIDTRC incidents, he noted that;

> *"The impact of IIDTRC consisting of losses from disruption caused by an arrest without police cooperation harms the relationship between the employees and security managers".*

Reflecting on this response one can deduce that lack of interest shown by the police in investigating IIDTRC creates a serious challenge for security managers in the retail companies. This observation corresponds to suggestion of Walker *et al.,* (2009) that police indifference in cooperating with retail managers in combating IIDTRC has much impact on business organisation than the loss accrued through the loss of their business assets. However, Bamfield (2012) suggests that the issues of police indifference linger in the retail companies because the police often criticise retailer's crime prevention policy. And, in particular, that prevention of crimes (IIDTRC as it in this research) requires specific crime prevention policy changes for the retailers to receive substantial police cooperation. This suggestion by Bamfield (2012) supports Seneviratne (2004) arguments that police should be liable to their own decision whether to adopt a particular policy or prosecuting a perpetrator. And that it is the responsibility of the police to post their men to crimes incident, but in whatever crimes detection and prosecution, police are not the servant to anyone, except for the law itself.

Interestingly, these arguments tend to defend the police indifference in investigating of crimes and also points to the reason behind the attitude of the police regarding their indifference in preventing IIDTRC.

In addition, Bamfield (2012) suggests that other issues such as individual decisions, corporate culture, operational shortages, may contribute to the police indifference attitude in preventing IIDTRC in the retail companies.

Retail companies are not alone in facing the challenge of police indifference in their effort to prevent IIDTRC. The Confederation of British Industry (CBI) in 2010 Report (*A Frontline Force: Proposals for More Effective Policing*) suggests that there are concerns about police inefficiency in crime prevention across business sectors. The concerns are worsened by other related issues such as police costs, weak strategic police leadership, inefficiency in their organisational structure and complexity of dealing with crime investigation where police spend lots of time dealing with minor crimes cases (Carter, 2003; Berry *et al.,* 2009; CBI, 2010).

The Home Office (2011a) policy statement (*A New Approach to Crimes*) raised similar concerns about police indifference in getting grips with the prevention of crimes. Comparatively, the CBI's report and Home Office's policy statements seem to defend the ways things are being done in the police. They argue that the issues of inefficiency and bureaucracy in particular within the police contribute to their indifference attitudes towards crime prevention.

Notwithstanding that bureaucracy exists in every institution that deals with crimes (Bamfield, 2012), it is vital that police should have a specific ways of dealing with IIDTRC in the retail companies. There should be a procedure agreed upon by both the retail management and police to minimise the issues of bureaucracy in investigating and prosecuting the IIDTRC perpetrators. Provision of clear roles and responsibilities between the police and retail management would reduce the brick-wall that might be encountered by the police during IIDTRC investigation. Clarifying on the role of the both parties would reduce the amount of time spent on particular IIDTRC incident.

For instance, it could reduce the amount of paperwork regarding IIDTRC incident and witness reports. Consequently, clarifying the roles of the police would reduce the bureaucracy that might have given birth to indifference, which may curb the impact of the IIDTRC in the retail companies. However, this suggestion would only work effectively if there are an existing relationship and collaboration between a retail company and the local police. The *Head of Crimes Investigation* from *RetailGroup* noted the difficulty his management team faces in trying to build effective working relationship with the local law enforcement agency;

"When there is the change of the head of local area police, all the long built relationship, and working team would breakdown…, to build up a relationship with the new administration is not easy! Sometimes it is not easy to find the police officer that would play the role of effective investigation of IIDTRC…it is always a problem…it is, yes it is…this always lead to delays of investigation and prosecutions……"

This remark suggests that retail management needs to work collaboratively with the local police. Another option that would change the police indifference in preventing IIDTRC is to establish a system where the retail security officers and police would work together. This kind of system (*Project Griffin*) was initiated in the case of counter-terrorism where police, business and the private sector security, emergency services and local authorities are coordinated to protect UK cities from terrorism (Confederation of European Security Services (CoESS), 2012).

There should be law police enlistment of retail security officers to enable the retail security management work collaboratively with them in protecting retail information systems while preventing IIDTRC. Such collaboration ingrained with good relationship would enable the police to understand the retail operations, reduce the potential IIDTRC investigation bureaucracy and thus change the police indifference attitude in preventing IIDTRC in the retail companies.

6.3.2 Summary of Results from RetailGroup

The findings from the *RetailGroup* have provided an insight of the nature of internal identity theft-related crimes in a typical UK online retails company. In particular, the finding suggests that *RetailGroup* may understand the features of internal identity theft related crimes (IIDTRC); there are still challenges that require their management attention. One of the major challenges is the lack of clarity of management responsibility with regard to data security and prevention of IIDTRC. There is also an issue of unclear internal policy and varying understanding of data security related issues across the levels of employees. There are instances of varying security strategies attributed to the nature of the crimes, the law enforcement indifferences to issues of IIDTRC and cultural orientation of the perpetrators. These varying issues and segregated data security roles weaken implementation of data security strategies. On the other hand, this case study suggested that training of employees is very difficult to achieve in *RetailGroup* due the time and cost associated implications.

RetailGroup may have incentives to invest the significant resources in training their IT security and crimes prevention employees, but budget constraints and operational changes are still the challenges to deal with. As a result, they continue to adopt coercive data security strategy approaches which pay off on short term basis.

However, while *RetailGroup* IIDTRC prevention issues may be an extreme case, perceptions of participants and findings discussed above cannot be considered complete representative of IIDTRC prevention management issues in the UK online retail sector. The purpose of this case study was not to identify all the features of the nature of IIDTRC and the complete list of IIDTRC prevention challenges in online retail companies. It was used to bridge of the research gaps identified in the literature review above.

In addition, the findings from the *RetailGroup* provided the background for the confirmation of the assumptions that was conceptualised by the role-based framework (RBF) in chapter 3. Since this analysis is limited to the context of *RetailGroup*, it was used explore and generate some significant issues for further investigation.

To investigate on how the retail management could minimise the impact of these IIDTRC prevention challenges, the RBF approach was applied in analysis of the information security audit conducted in the three retail companies: *Xtail*, *Ytail* and *Ztail*. The next section provides the results.

6.4 Results from Xtail, Ytail and Ztail: Cross Case Analysis

This chapter analyses the data from *Xtail*, *Ytail* and *Ztail* collected through participant observation and convergent interview. The practicalities of participant observation have been discussed in section 5.3.3.5 and manual content analysis, as discussed in section 6.3 above, was used for the convergent interview. The cases of *Xtail*, *Ytail* and *Ztail* were used to extend the application of role-based framework. Yin (1994) and Huberman and Miles (1994) suggested that that investigating multiple cases enables the researcher to build a logical and multiple chains of evidence to establish theoretical assumption. Hence, this chapter identifies the chain of evidence for the analysis of all the cases on the basis of the Role-based framework. This section investigates the RBF proposition that:

- *Collaboration of the management has impact on the management roles (IS/T and crime prevention) in prevention of IIDTRC; and*
- *The collaboration of management roles has an impact on the implementation of tools required for the prevention of IIDTRC.*

Thus, it provided the answers to the research questions 2a and 2b in the chapter 1 of this study respectively:

- *To what extent do the attributes of the framework influence the internal identity theft related crimes prevention practices?*

- *To what extent do the IS management influence the effectiveness of identity theft related crimes prevention framework implementation?*

The investigations were based on: how robust are the conducted Information Security Audit (ISA) evaluation, measured on the three key criteria – time, logistics, effectiveness; does it meet the objectives of intended auditee company? What was the relationship between the auditor and auditee compared to the status quo? Was there anything new compared to what the auditee was used to?

The taxonomies of the related findings to these questions are presented in tables with respect to *Xtail*, *Ytail* and *Ztail*, and results of the cases are interpreted in relation to their commonalities and their differences. This approach enabled the researcher to focus on the status quo of the auditee past audit practices and compare them with what was observed. Hence, the generated codes from the interviews and results from the observation were compared to provide a comprehensive research results.

The researcher analysed collated data based on the stipulations of ISO 19011:2011 described 5 above. However, in some procedures where convergent interview were impractical field notes were used to capture critical data regarding the authority expressed by the participating companies.

6.4.1 Management Collaboration for IIDTRC Prevention in Xtail, Ytail and Ztail

To investigate the extent to which *Xtail*, *Ytail* and *Ztail* management collaborated to discharge their responsibilities of information systems audit given the potential for internal identity theft-related crimes in their companies, the researcher evaluated the following ISA main procedures based on the stipulations of ISO 19011:2011.

Cases	Management Position	ISA Approach	Approx. Auditing Duration	
			Investigation	Implementation
Xtail	Head of IT Support IS Security Auditor	Joint Party (internal + external + Researcher)	3 days	4 days
Ytail	Operations Manager Account General Manager	Second party (External Only + Researcher)	7 days	10 days
Ztail	Customer Acct Manager Internal ISA	First party (Internal Only + Researcher)	5 days	8 days

Table 40: ISA Team and Duration of Cases (*Xtail*, *Ytail*, *Ztail*)

The findings from *Xtail*, *Ytail* and *Ztail* reveal that their management recognise the importance of the Information Systems Audit (ISA) needed to protect their customers' data from Internal Identity Theft Related Crimes (IIDTRC) and data leakages Table 40 shows the respective companies (*Xtail*, *Ytail*, and *Ztail*) with the participant's management position, ISA approaches and approximated auditing duration.

IS security priority areas investigated	Are they Applicable to the Companies?		
	Xtail	***Ytail***	***Ztail***
Legal and data Protection	Yes	Yes	Yes
Data	Yes	Yes	Yes
Disposal	Yes	Yes	Yes
Business Continuity	Yes	Yes	No
Data Field	Yes	No	No
Physical Security	Yes	Yes	Yes
Personnel	Yes	Yes	Yes
Websites	Yes	Yes	No
Network	Yes	No	No
Infrastructure (Laptops, Logical Access, Servers)	Yes	Yes for Laptops; No for Servers and Logical Access	No
PCI	Yes	Yes	Yes
OfCom	Yes	Yes	Yes

Table 41: ISA Priority Areas in *Xtail*, *Ytail*, and *Ztail*

The use of the collaborated ISA approach by *Xtail* was been boosted by the audit team members – IS security auditor and head of IT support, where the essential skills were applied to provide satisfactory ISA assessment. However, *Ytail*'s and *Ztail*'s scopes of using the audit team comprised of customer account management led to protracted audit duration; since the customer account manager could not provide answers to the technical IS/IT security related risks. This issue of using an unskilled audit team that was unaware of emerging ISA techniques resulted in non-assessment of some IS priority areas (as shown in table 41 above) which may pose IIDTRC risks.

The *Ytail* and *Ztail*'s lack of Information Security (IS) investment justification centred on investing in respectively second party audit and first party audit might have been appraised using the collaborated ISA approach adopted by *Xtail*. For instance, timely audit planning, satisfactory audit criteria, comprehensive audit scope and organised audit team (although acknowledged in some cases *Ytail*) were not readily meet by *Ytail* and *Ztail*. Hence, to investigate the extent to which *Xtail*, *Ytail* and *Ztail* management collaborated to discharge their responsibilities of information systems audit given the potential for internal identity theft-related crimes in their companies; the researcher evaluated the following ISA main procedures based on the stipulations of ISO 19011:2011:

i. Audit Plan
ii. Audit Criteria
iii. Audit Scope
iv. Audit Team
v. Audit Duration (Time)
vi. Audit Findings
vii. Audit Conclusions

Audit Plan: For the *Xtail*, the planning was timely and detailed. Both the auditor and auditee cooperation was smooth. The verification by the external auditor noted that the necessary resources were available and the needed tools were in place. As for *Ytail*, the necessary planning was done by the external auditor. The expected completion date for the auditing was extended. Most of the auditing tasks were left to the external auditor. In *Ztail*, though the planning was timely but did not meet compliance requirements because it was limited to the objectives that were only applicable to the auditee. The internal auditor in *Ztail* noted that their practices were based on the stipulations from the *Ztail* top management.

Audit Criteria: *Xtail* met all audit criteria. The resources (technical and human) were identified and put in place before the commencement of the audit. The objectives of the audit activities were clearly defined. All the policy documents were complete and were up to date. The audit compliance requirements were met. The last audit conclusion and the implementation made after that was presented. In *Ytail* the policy documents were not available. In some cases, they made calls to request for the documents. Some of the issues related to role clarification – *'who does what'* extended the audit programmes duration. The management of the *Ytail* was not coordinated.

The audit personnel records were not established and maintained. The visiting data compliance manager noted that change is required to the IS management. Similarly, for the *Ztail*, the relevant ISA documents were available. Audit criteria were reserved for security infrastructure and issues that would benefit their company.

For instance, there is no policy initiated by the company that covers 'Data Field', 'Business Continuity', 'Network' and 'Server' element of 'Infrastructure' (as marked No in table 46 above). The auditee customer account manager noted that '*Ztail*' is only concerned about the data they pulled from the main server. Since they do not store the customers data on their system – 'make use of only the pulled data'; it is the responsibility of the IS security management in their head office. This observation was noted as a major issue.

Audit Scope: *Xtail* presented a comprehensive organisational chart showing the responsibility of each component. The platform was set for the audit activities. The contribution of the head of the IT Security support combined with the internal auditor was good. In *Ytail*, although there was apparently 3 weeks of notice before the audit commenced, there was no arrangement put in place that explains the organisational structure. For instance, the HR office was locked for hours when we visited to ask for the policy covering 'sacked employee leaving procedure'. Similarly, we could not get access to infrastructure, data field information, etc. (as marked No in table 46). The *Ztail*'s management structure was well presented. They went far as ensuring that all the necessary management team was available when needed. We observed that the internal auditor had prepared the management team ahead of the audit. This was noticeable from the body language of some of the management. There were panics, disarray and jittery in some cases.

Audit Team: In the same vein, *Xtail* recorded the as the best audit team. They had a comprehensive audit plan and audit criteria. The team communication was smooth.

Xtail's audit team had good knowledge of the organisation structure and units. Technical support was available throughout the audit activities and programme.

In the case of the *Ytail* communication between the operation manager and customer account manager was not coherent. There were cases of shifting responsibilities. For instance, when asked about their Payment Card Industry Data Security Standard (PCI DSS) compliance, their reactions show that they do not know the consequences of not being compliant to PCI. The external auditor noted the issues as high risk and was reflected in their audit report. They were asked to treat the issue with urgency. Although there was smooth communication at the earlier stage of the audit in *Ztail*, but it started to break down at the investigation and document review stage of the audit. The internal auditor relinquished most of the responsibilities to their companies head office. Some of notable non-compliance issues we observed were shifted to the responsibility of the top management. The team always tried to avoid taken responsibility for IIDTRC risk issues raised.

Audit Duration (Time): It took approximately 7 workings days for the audit in *Xtail* – including the time for the implementation IIDTRC risk issues, feedbacks, audit reports and conclusions. This excludes the time for the notification of the audit appointments and preparations. This observation reveals that it took almost one-fifth of the audit duration for *Xtail* to complete the ISA tasks, even to some level of satisfaction. In *Ytail*, it took about 17 working days to sort all audit issues: from implementation to the feedback. In some cases, the external auditor coerced the *Ytail* with a strict deadline. Not as much longer in *Ztail*, it took about 13 working days to implement all the notable recommendations noted in *Xtail* and *Ytail*.

Audit Findings: *Xtail* made the IS Security Priority Areas (shown in the table 46 above) available for investigation. Most of the colour coding was shown in green with few in amber. This shows that there was a low risk of IIDTRC related issues. In contrast, *Ytail* could not provide answers to areas such as 'Data Field', 'Websites', 'Network' and some elements of the 'Infrastructure' (Logical Access, Servers). Similar to *Ytail*, *Ztail* could not provide security assurance on the following: Business Continuity, Network, Data Field, Websites, and Infrastructures.

Audit Conclusions: The observation from *Xtail* above revealed that Xtail conducted a robust ISA in the prevention of IIDTRC, having met all the audit objectives with all the IT essential IT security tools and resources made available.

As for the *Ytail*, their approach and audit procedure were poor. Most of the responsibilities were left for the external auditor. It would lead the company to spend more for the audit since it involves a protracted period due to delays and poor planning. Similar to *Ytail*, the *Ztail* audit team was protective in their approach. This perception affected the audit objective. There were issues of inconsistencies and shifting responsibilities on the significant IIDTRC risk issues.

6.4.2 Factors that Influence the ISA Performances in the Xtail, Ytail and Ztail

The use of convergent interview to investigate what have influenced the performance of *Xtail*, *Ytail* and *Ztail* in their used of the Information Systems Audit (ISA) to prevent Internal Identity Theft Related Crimes (IIDTRC) revealed the following key factors;

- Clarity of Auditors Roles
- Audit Attitudes and Auditors Perception
- IT Security Knowledge

Clarity of Auditors Roles: Clarity of Auditors Roles was mentioned as being vital to the performance of *Xtail*. For instance, the Head of Security Support in *Xtail* stated:

> "*Auditor should be explaining what security controls are in use in their auditee companies, and why the controls, prior to the start of security audit…"*

On the other hand, the security auditor in *Xtail* agreed with Head of Security Support and expressed her displeasure with the quality of external auditor contracted to their company. She noted that it is important that the information security auditor should be very clear in explaining what is needed to be reviewed and why. These statements from the *Xtail* suggest that organisational structure may have an effect on the auditor's performance their discharge of their roles and responsibilities.

Audit Attitudes and Auditors Perception: Both auditors and security professionals noted that auditor's attitude and perception about the role of ISA in the prevention of internal identity theft related crimes were important. In response to question of his perception in collaborating with auditee, the external auditor in the *Ytail* stated that;
"Although this is not always the case, with my experience most of IT security professionals in the auditee see us as collaborators..., this experience has made me believe collaborating with professionals helps to take effective review of security issues and tries to integrate system-wide to leverage existing human and IT resources, …"

In contrast to this view, when the operation manager at *Ytail* was asked why there is no IT/IS professional in their audit team, he answered that;

> *"....it is the job of the external ISA auditors...., we paid for these issues to be sorted by them (external auditors)…one thing about most of these auditors...or such bodies…is that they can never be pleased...though some of them are very easy to get on with…sometimes you won't be lucky to have nice ones around…"*

This statement suggests that some of the auditee companies are left with no option than to abandon their companies ISA or related checks to the regulatory bodies. In addition, these statements suggest that there is a perception of low expectations of ISA services by this manager and also that paying for ISA services might be enough for their company's data security. This perception that paying for ISA checks to the external bodies is enough for effective internal data security seems to contribute to the poor audit performance observed in both cases (*Ytail* and *Ztail*). It also shows that attitudes of some external auditors in auditee companies could bring negative impact to the audit performance. This suggests the reasons for the lack of planning, inconsistencies and lack of cooperation between the external auditor and audit team.

Information Systems Security Knowledge

The influence of Information Systems Security Knowledge on the performance of *Xtail*, *Ytail* and *Ztail* in their used of the Information Systems Audit (ISA) to prevent Internal Identity Theft Related Crimes (IIDTRC) is based on *Xtail*'s audit scope. *Xtail* utilised the expertise of their head of IT security support and matched his role with their internal auditor to create a strong internal IS control system. The audit team brought the potential IIDTRC risks in there at the forefront of the external auditor and demonstrated the strategies on which they are working to resolve the flaws. This practice enables both the external and internal auditor to work cooperatively and timely to resolve the potential IIDTRC issues.

From the investigated practices of *Ytail* and *Ztail*, there are ISA issues related to poor planning, inconsistencies and shifting of responsibilities in either case. These issues have a great impact in meeting the aims and objectives of the ISA. It put a question mark on the relationship between the auditors and auditee companies. In both cases, the auditors shifted their responsibilities to the companies' management team. They are entangled in the perception of seeing their workings of the ISA as *status quo* routine services. These practices affected their performance of the audit checks.

In both cases, the IS priority areas were unchecked because '*there was no one'* answerable to these issues. The loopholes that pertain to these unchecked priority areas pose high potential risks of IIDTRC and data leakages to both companies; compared to the observations from *Xtail*. This observation shows, perhaps in case of *Ytail*, that members of the team did have much knowledge of the IT/IS security related issues.

6.4.3 Impacts of ISA Approaches in IIDTRC Prevention in Xtail, Ytail, Ztail

The outcome of the investigation on how robust the Information Security Audit (ISA) conducted in the cases meets the objectives of audited companies was analysed based on the three key criteria: time, logistics and effectiveness. The finding from the comparative analyses of *Xtail*, *Ytail* and *Ztail* suggests that cost reduction and internal security control were identified as the major impacts of using different ISA approaches in the prevention of internal identity theft-related crimes.

Cost Reduction Benefits: The use of first party audit and second party audit in respective cases of *Ytail* and *Ztail* allowed for the perceived ISA cost benefits of not paying for the IT management. However, subjectively, these companies incurred indirect costs of protracted audit duration and potential IIDTRC risks compared to *Xtail*. *Xtail* utilised the combined support of their Head of IT security, security auditor and the external auditor to ease the burden of audit roles and responsibilities. The ideal of combined support enabled *Xtail* to prepare the audit plan in advance to the meet the audit criteria and expected targets. When the internal auditor of *Xtail* was asked about their roles in meeting the objectives of the audit criteria, she noted that her audit team knew the inspection process in advance. In her words,

> "*We would always check the previous examination manual and audit checklist. …in some cases, we do obtain the documents from the IS security audit regulatory body. Besides, we often attend some ISA professional workshops. These practices prepared us ahead to work with the external auditors as this…"*

This statement suggests that *Xtail* audit team has good knowledge of the changes in their company and IS business environments. *Xtail* have endeavoured to enforce and update recommendable priorities within the audit regulatory agency. This attribute facilitated their audit performance and provided room for suggestions and new requirements. They were open to accommodate new ideas by detailing some of the problems they had in the past and how they tackle them. This demonstrated their level of integrity and competence, not only to the external auditor, but to the *Xtail* as their organisation.

Benefit of Internal Security Control Assurance: It was observed that sound internal security control attributed to *Xtail*'s robust practices of meeting audit criteria. They presented audit log documents and follow-up processes were established while ensuring their audit compliance and proactive check to IIDTRC risks. *Xtail*'s audit team also noted that the absence of evidence for the internal audit programme could be a sign of deficiency and such an issue can create bias between them and the visiting auditor. It might extend the audit duration and incur more costs, not only for the auditor but also for the logistics – disruption of business activities. *Xtail* noted that using a collaborated audit approach pays in reducing the IIDTRC risk as it avails the opportunity to leverage on the audit skills lacking in their company. It is availed them to the audit assessment tools such as software to meet the advancing IS/IT world. The *Xtail*'s head of IT security supported this view while discussing their audit plan, he noted;

> "…Y*ou don't have to be spending money on every IT programme and chips…they are money……in some cases it doesn't worth investing…."*

This statement suggests that the management of *Xtail* is still reluctant in investing in improving their IT security programme, and that some of investment on the effective internal security tools do not worthwhile.

6.4.4 Summary of Xtail, Ytail and Ztail Cases Analysis

The analysis of the results across the cases draw a line between collaborated and independent audit approach which weigh how the management of *Xtail*, *Ytail*, and *Ztail* prevent internal identity theft related crimes (IIDTRC) based on the evaluated audit practices – plan, criteria, scope, duration, etc. The approach of the collaborated audit observed in *Xtail* provides ISA team with an assurance that the audit report, efficiency and effectiveness of the audit operations are in compliance with ISA regulations. The result has suggested that the collaborated ISA approach adopted by *Xtail* enhances the management effort in building a strong work ethics that was shown by their level of integrity and competence. And this is evidence by their performance in meeting the information security requirement in the prevention of IIDTRC.

In addition, the collaborated ISA approach enabled the *Xtail* audit team to detect loopholes in their IT security systems and tackle them effectively.

Collectively, these attributes of collaborative ISA suggest that a directed the management effort established in the *Xtail* provided them with an effective internal security control and improved risk assessment against IIDTRC. These findings suggest that if the management can take control of internal IS security issues, it would ease the ISA procedures, reduce the audit time and cut down logistics.

The collaborated ISA approach can also promote the sharing of security expertise and IT skills that can contribute to effective ISA in the prevention of IIDTRC. It vital to note that collaborated ISA idea enhances the chance to identify IIDTRC risks as evidence in the case of *Xtail* which have shown that integration between audit and IT security management at *Xtail* contributed to robust ISA. In contrast, in the *Ytail* and *Ztail* where the audit practices and management roles sharing functionality were not collaborated, the impact of ISA in IIDTRC prevention could not be realised. Collaboration can make it possible for management to share their roles/responsibilities in relation to IIDTRC prevention, thereby improving the likelihood that effective IIDTRC prevention implementations. The analysis of the results from these cases suggests that effective information security audit in relation to the prevention of IIDTRC depends on the collaboration of management effort and roles. The IIDTRC prevention requires that the management efforts and roles among the IT security and crime prevention management should be shared with one another.

6.5 Summary of Data Analysis and Results

This chapter has provided an analysis of the result of the data collected from the archival cases and selected cases: *RetailGroup*, *Xtail*, *Ytail*, and *Ztail*. The findings from the archival analysis have provided evidence that corporate and personal identity theft related crimes perpetrated through account take over and account withdrawal as the common in the online retail sector. The findings from the *RetailGroup* provided some results which complement the results of the archival cases. Though, there were some issues the respondents passively addressed. For instance, there was no information from the *RetailGroup* to indicate the number of cases of IIDTRC in their organisation. They also avoided providing answers the nature of IIDTRC prevention tools they are using in their organisation. Perhaps, these issues were passively treated due to security concerns. The results from the *RetailGroup* has provided insight about the challenges faced by the IS security management on implementing IIDTRC prevention strategies.

The results showed that challenges identified here were encountered by the IS security management, as an individual and as a team in carrying out their IIDTRC related roles and responsibilities. In addition, the findings from the *RetailGroup* has provided the empirical background on how the RBF attributes could be applied to managed the identified challenges.

The findings from the *Xtail*, *Ytail* and *Ztail* have shown how the management can use the collaborative concept of role-base framework (RBF) to tackle the identified challenges. As a complementary evidence, the results of the cases (*Ytail* and *Ztail*) confirmed the basic evidence of the challenges IS security face as identified in *RetailGroup*. The comparative analyses of these cases showed that collaborative roles sharing could improve the likelihood of the management performance in implementation of IIDTRC prevention practices.

Xtail case indicated that collaborative roles sharing the attribute of RBF could enhance IS security management performance in the IIDTRC prevention. That is, it provides the answer that there is a likelihood of the impact of collaboration of management on their performance in implementing their roles and responsibilities in relation to IIDTRC prevention. These findings cases provided the insight on the important of RBF attributes of collaborative roles sharing. This triangulation of empirical evidence on the nature of IIDTRC and application of role-based framework in relation to internal identity theft related crimes prevention in online retail companies provide the background for the discussion in chapter 7.

CHAPTER 7

RESEARCH DISCUSSION

This chapter discusses the results of the study. It relates the findings to the empirical suggestions reviewed in chapter two. It provides critiques of the findings and discusses how the research results differ or agree with past empirical studies done in the areas of identity theft prevention. Based on the findings from chapter six, this chapter extends the discussion of the place of the role-based framework (RBF) in the prevention of the Internal Identity Theft Related Crimes (IIDTRC) in online retail sector. The discussions are presented in four sections.

First, it provides an overview of the study, including a problem statement and major methods involved in this research. Second, it discusses online retail as a site for understanding the multi-faceted nature of the IIDTRC. Third, it discusses the challenges identified in chapter six that impact on the extent to which management act in preventing IIDTRC. Four, this chapter discusses benefits and implications of using RBF to tackle the identified challenges. Majority of this section is devoted to a summary and discussion of the four RBF propositions. And this concludes the discussion of the pertinence of the results of the role of security management in preventing internal identity theft-related crimes in online retail.

7.1 Summary of the Research Problem and Methodology

Internal Identity Theft Related Crimes (IIDTRC) in e-businesses has risen by nearly 60 per cent in five years across UK. Over 230, 000 cases of IIDTRC and employees related frauds were recorded in England and Wales from January to June 2014 (Office of National Statistics, 2014). British Retail Consortium (BRC) (2013) and Kroll Global Fraud Report (2013) placed the UK online retail as one of e-business sectors where the IIDTRC are prevalent with the IIDTRC incidents rising to 80 per cent compared to other retail frauds. As the IIDTRC incidents are increasingly impacting the socio-economic, cultural and managerial fabric of the online retail, urgent efforts are being made to strategize all possible security resources – human, technological and process – to prevent the recurring incidents. All the strategies and tools that are increasingly being mobilised in the prevention of IIDTRC are placed as the roles of online retail security management.

The assumptions are that security management is ideally positioned;

- to reach employees as well colleagues in developing the essential skill to prevent IIDTRC,
- to play an important role in providing essential data security information, and
- to implement essential security tools and/contribute to attitude change that will allow retail companies to protect their Information Systems (IS) infrastructure.

Information Security management are considered the 'window of hope' in preventing the IIDTRC because of their statutory jobs roles of ensuring effective data security against data theft and data leakages (ACFE, 2014). Along with data compliance management, human resource management and law enforcement agencies, information security management are assumed to have essential skills required to integrate people, processes and technology for prevention of IIDTRC in online retail companies (Valrie and Rabih, 2013). In spite of this important role of information security management, however, the bulk of the research on identity theft prevention has focused on generic preventive strategies and tools rather on the management themselves that implement the tools.

A few studies have examined the current and potential role of security management in the prevention of IIDTRC in a defined business setting like online retail. And, in general, there appears to be an implicit assumption on the part of practitioners in information systems that provided management are given clear roles and are collaborative in prevention of IIDTRC, they will – regardless of their individual management roles – ensure that security tools are implemented effectively to protect online retail companies' IS infrastructure.

The overall purpose of this study was to provide a framework for prevention of IIDTRC in online retail companies and to understand how the framework can be applied to the online retail IS security management. In this manner, this study sought to fill the gap in the research on roles of IS security management in the identity theft prevention which has typically focused on cataloguing IIDTRC prevention strategies, but without relating them directly to management practices and roles. The assumption of this study was that a better understanding of the nature of IIDTRC in online retail and the contextual practices that influence management collaboration in carrying out their roles could provide a key input into the design of practical strategies that will strengthen the management performance of IIDTRC prevention.

Acknowledging that the integration of practices and theories in studies of IIDTRC in online retail setting is generally lacking (Kardell, 2007; ACFE, 2014), Role-based framework and organisational role theory were used as basis for the inquiry into collaborative roles of management in prevention of IIDTRC. Other important issues which could impact roles of information systems security management were identified and operationalized in the course of this study based on an extensive review of the extant literature as well as on the interview discussions and observations in the data collection phase. In this manner the following issues were identified as possible predictors of management impact to prevent IIDTRC in online retail; understanding of the nature of IIDTRC, challenges of preventing IIDTRC, and collaborative roles sharing in implementing of IIDTRC prevention practices. Previous studies have typically examined identity theft prevention in online retail from the perspective of generic framework intent (built on the external factors and on the concept software security); neglecting the unique operationalizing nature retained by every business sector, internal activities of the employees and impact of management roles.

However, discussions with the management during the data collection phase of this study had However, discussions with the management during the data collection phase of this study had indicated that prevention issues of the identity theft related crimes was context specific, involve either external and internal of activities of employees or combination of both, and could be built on the collaborative roles of all the management – human resources, information systems security and crime prevention. This study thus departed from the approach taken by other studies by operationalizing the predicted management issues 'collaborative management roles for IIDTRC prevention' in terms of three major issues: understanding the nature of IIDTRC in online retail, the clarity of management roles and practices in prevention of IIDTRC, and collaboration of the management in implementing the security tools and strategies.

These issues underpin the concept of role-based framework (RBF) which assumes that the integration of management roles in a collaborative approach would be beneficial in implementing IIDTRC prevention practices. In practice, however, the literature review has shown that management role collaboration is affected by number of attributes including people, operations, processes, organisational roles, and technology and management characteristics. These factors also have also been shown in the previous studies (e.g. Biegelman, 2009; Shah and Okeke, 2011; Steinbart, Raschke, Gal and Dilla, 2012) to be relevant to the success of information systems (IS) security in organisations.

Hence, the applicability of RBF was evaluated through the field work to investigate if effective IS security as being argued by the suggestions of these previous is likely to be subjected to clarity of integrated shared roles the IS security management uphold. This study was conducted in the Northwest of UK among the management of online retail companies. A non-experimental qualitative research design was used to examine the difference issues that were identified as being potentially important to security management in preventing IIDTRC. Data were obtained by conducting interviews containing predominantly structured questions in four selected companies. Although the study was conducted mainly through interview, participant observation techniques were used to: inform the study framework evaluation phase; to aid conceptual framework extension; and to assist in the clarification and interpretation of the results of this study. This study was conducted in two phase.

The – archival analysis – phase took place over a period of eight weeks between the months of December 2011 and April 2012. During the archival analysis, examples of individuals who have been caught attempted to and/or engaged in internal identity theft related crimes and frauds were discussed based on their age (at the time of the fraud), gender, job title/e-business sector, description of the nature of the fraud (attempt), motivation, how caught and lessons learnt. The second phase took place from May 2012 to September 2012, and covered 20 weeks period during which semi-structured interview were conducted (with 12 security and crime prevention managers) as well observation of six information security audit personnel. In addition, convergent interview was conducted with the six security information audit personnel.

7.2 Online Retail as a Site of Internal Identity Theft Related Crimes

The finding shows that online retail customers are not only victims of IIDTRC. The online retail companies suffer a great impact from these crimes. The archival result shows that stealing of credit and debit card details, corporate and personal account manipulation and account withdrawal are major identity theft crimes in the retail sector. This finding agrees with research reports (e.g. Kroll, 2011; CIFAS, 2012) that customers' payment card numbers and details are the major targets. It also agrees with the suggestions by Hinds (2007) and Mitnick (2002) that data tampering and copying are key methods of carrying of IIDTRC.

These suggestions indicate that corporate account details are also at risk as customers' personal identifiable information (PII). The impacts from IIDTRC are inestimable as suggested by the examples of the cases of individual that were caught; although the indicators of the impacts of IIDTRC incidents are not released to the public may be due to the privacy-related issues as it was seen in the archival analysis that some of the cases were not in the public domain (Hastings and Marcus, 2006). This finding agrees with the suggestions by other researchers (e.g. Stickley, 2009; Hurst, 2010; Shah, Okeke and Ahmed, 2013) that companies might not be encouraged to reveal the impacts of IIDTRC as such publicity might bring some irreparable dent and damages to their companies' brand. This issue of protecting the victim companies' brand and reputation is one of the major factors that have led to increasing incidents of IIDTRC in online retail sectors. Without reliable data on IIDTRC incidents, it would be difficult if not impossible to provide a contextual IIDTRC preventive measure (Laudise, 2008).

Other factors that were identified as the major factors of increasing IIDTRC in retail sector include;

- Retail business operations;
- Over-dependency of information security management on software security;
- Perceptions of the nature of IIDTRC in online retail;
- Lack of IIDTRC incidents analysis;
- Absence of human-centred security in online retail;

Lack of reliable data about internal identity theft-related crimes incidents:

The finding of the archival analysis was based on the few available data at the public and private research domain. This unavailability of data arises from three causes: online retail companies rarely share data on IIDTRC incidents; online retail companies gather data on IIDTRC incidents for narrow purposes and; IIDTRC perpetrators always act to conceal their trails. First, IIDTRC incidents data are withheld due to concern over brand reputation, copycat activities and publicity. Perhaps, also due to privacy related issues. Few available data were shared under guarantees of confidentiality and under restricted-use agreements. IIDTRC incidents data are only available if there is no other option. With these limited access issues, IIDTRC incidents data discussed here were rarely available to the researchers. Second, the retail companies have no motivation to share data on related to IIDTRC incident. They are only provided for selected cases of forensic investigation or legal proceedings. Sometimes, the available data were not organised. In some cases, the databases were not accessible. These issues made the archival collation and analysis bit intensive research.

Third, most of the IIDTRC perpetrators are skilled enough to cover their trails before the detection. In some cases, it takes a short period of time to carry out a successful attack. Perpetrators often devised and conceal their perpetration trails. These issues contribute to incomplete data capture on their methods of their IIDTRC threats. This was noted by researchers (Newman and McNally, 2005) as one of the setbacks of identity theft prevention research. However, this study used this archival analysis strategy to deliver valuable insights despite the deficiencies in the data material.

Retail business operations: The archival analysis suggests that retail business operations are one of the major factors that accounts for the increasing cases of IIDTRC in online retail. The case examples analysis suggest that the use of credit and debit cards through mobiles phones have encouraged successful perpetration of IIDTRC in online retail compared to other sectors (Meulen, 2006; Forrester and Seeburger, 2013). In particular, the archival analysis suggests that desk-based employees that carry out most of the end-user online trading through credit or debit cards are more liable to IIDTRC than employees from other departments. This trend is followed by finance/accounting operation employees and upper executive management. These findings suggest that most employees in online retail operation are a potential threat to the identity properties because of the situational or the opportunistic nature of that their job roles.

The findings suggested that more attention should be given to the operational departments, IT departments and management positions, other than to age and gender. Thus, these findings suggested that the characteristics of the IIDTRC perpetrators are not likely to be classified based on gender but on their operational departments and management. This contradicts the suggestion by the CIFAS (2010) that youths have more tendencies to indulge in IIDTRC than adults. In addition, the finding from the archival analysis suggests IIDTRC perpetrators are not likely to be categorised based on their genders. For instance, from the archival analysis, the age of perpetrators span across late 20s to late early 50s, and there was almost no significant margin between the numbers of male or female perpetrating IIDTRC in the business organisations.

Over-dependency of the retail information security managers on software security

This issue of management relying too much on the software security for prevention of IIDTRC was confirmed in the archival cases analyses which suggest that management of the companies leaves the activities of the employees to be monitored by security systems.

This is one of the major issues since the information systems are designed by some of the employees, the perpetrators may be as skilled as those that designed the security software. For the instance, the case of 'Mr. Smith' in the archival analysis cases, a software engineer who stole the customers' card details for his financial gain. The detection capability of software security cannot match the effectiveness of the use of monitoring and security audit as have seen this example of 'Mr. Smith' because he has the skills to cover his fraud trails.

This finding agrees with the study by Allen *et al.,* (1999) and Hofmeyr, and Forrest and Somayaji, (1998) that there might the need for the contributions of the software security in preventing IIDTRC but cannot equate the human security through monitoring and security audit. In addition, this finding suggests that over-reliance on software security creates the perception that adequate security are in place. This perception is misleading in a way the IS security management neglect the implication such as – the cost of maintaining software, updating them and technical-know-how. These findings suggested that the way forward for effective internal data security is by developing and empowering the end-users through human-centred security such as monitoring and security audit.

Perceptions of the IIDTRC perpetrators in online retail

The management from the *RetailGroup* often referred the perpetrators of IIDTRC as the employees from the operational departments – call centres. The management that were interviewed perceived themselves as the 'clean employees' that rarely indulge in IIDTRC. This perception of varying understanding of the contextual issues of IIDTRC was suggested by Raab (2008) that different business organisation stakeholders perceive IIDTRC differently. Johns (1987) and Thompson and Mchugh (2009) agree with this suggestion and that the perceptions of seeing low-level employees as the potential IIDTRC perpetrators cause gross negligence of the top management who use their position to perpetrate these crimes.

Researchers (Koops *et al.,* 2008; Josselson and McAdams and Lieblich, 2006; Newman and McNally, 2005), have suggested that the varying concept of IIDTRC is one of the major setbacks of IIDTRC prevention. This study has reaffirmed that these varying concepts might be resolved by sector-based research on IIDTRC prevention, as done in this research. Perhaps it is through sector-based research like this online retail case that these issues could be rectified and resolved holistically.

Lack of IIDTRC incidents analysis: Another notable finding from this *RetailGroup* is that it has apparently no culture of crimes incidents analysis or strategy assessment. The management accepted that the prosecution of criminals closes the particular crimes incidents case. They noted that the IIDTRC case reports are documented for meeting reports but not really for analysis and assessment. They also believe that reoccurring incidents of these crimes avail them the opportunity to get experience on the intricacy of such crimes. This is contrary to the suggestions of RBF which emphasizes the importance of crimes incident assessment. RBF suggests that effective crime incident analysis and assessment reduces the risks and costs of similar crimes in the future. It also serves as a model or a clue for the crime prevention management. In agreement with the RBF recommendation, McLaren *et al.,* (2011) noted that for organisation to compete in a highly dynamic security marketplace, they must frequently adapt and align their security strategies and information system by continuous strategy analyses.

Some researchers (e.g. Lu and Ramamurthy, 2011; Ransbotham, Mitra and Ramsey, 2011), have also pointed out that that IT assessed security capability and empirical examination of vulnerability data disclosure mechanisms are enablers of firms' agility against any security threats. These strategies boost business organisation's security proactive stance and decrease the volume of exploitation attempts. Yet counter to these suggestions, the researcher found out that the crime prevention management in this study regarded experiences as the preferred method of improving their data security and crime prevention strategies, due to the cost of hiring experts or professionals to manage either their internal data security strategies or crimes incidents analyses. As also noted by KPMG (1997) and Ernst & Young (1998), prevention of IIDTRC requires effective data security risk management within the business organisations in which the analysis of the strategies adopted are in-lieu with the extent of the risks involved.

However, while these researchers suggest that it is the responsibility of management to educate employees on data security policy and that the analyses of crimes incidents cases are more likely to lead to effective prevention of IIDTRC, this research indicates that incident case analysis are not implemented due to some constraints such as finance, inadequacy of management, lack of strategy performance measures, inadequacy of management and employees' attitudes. Ekblom (2002) and Clarke and Eck (2003) noted that availability of resources, finance and staffing are among the greatest challenges of the crimes prevention within any socio-economic setting, even if there exist the clearer strategic crime prevention plans.

From this study, it was observed the management also faced the challenges of classifying the different types of IIDTRC risks/incidents. This view has a great impact in the allocation of the available resources. They struggle to determine priorities and areas of assistance in terms of immediate prevention action (low cost action and high risk/impact) and long-term interventions (deterrence law and penal reform, major policy changes and planning).

Absence of human-centred security in the online retail: The findings suggest that the human roles still play the huge part in preventing of IIDTRC in online retail. The 12 archival cases examples show that report from customers, law enforcement agencies and security audit are the methods through which the IIDTRC perpetrators were caught. These agree with the suggestions of Moore (2005) and Cappelli *et al.,* (2006), that the responsibilities of IIDTRC prevention lie with the human-centred security.
There is the need that concerns should also be directed to employees' operational policies and monitoring of the IS security infrastructure. It emphasises the need for retail companies to invest in employees training.

Researchers (e.g. Haagman and Wilkinson, 2011; Waker, 2006; Mercuri, 2005) suggest that employees' training is one of the vital instruments of IIDTRC prevention practice. The policy is very salient at any stage of IS security implementation of which without clear IS security policy the IT governance of the online retail would not hold water (Leon, 2008). Sommer (2012) and Meyers and Rogers (2004) suggests that an effective policy implementation is the root on which other IIDTRC prevention practices needed to be built on to achieve an efficient information security.

7.3 Lessons from Internal Identity Theft-Related Crimes Cases

The case analysis based on the profile of the individuals caught perpetrating IIDTRC provided a more general characteristics and additional insights of the nature of IIDTRC in the online retail. The IIDTRC cases describe variable such as age and sex of perpetrator and department of work/job role, but do not presume that this suggests a clear individual IIDTRC perpetrators characteristics that could be acted upon. Rather than retail companies infer the characteristics of the IIDTRC perpetrators describe in this research, the findings suggest the need to compare them to their individual company to determine if or/and why the same perpetrator may or may not depart from what was suggested in this case examples.

Based on the nine case examples analysed in the section 6.3 above, this research draws the following major characteristics of the IIDTRC perpetrators;

- *Perpetrators are not necessarily technical oriented to carry out IIDTRC.*
- *The nature of IIDTRC perpetrated by managers is comparatively different from IIDTRC by shop floor employees.*
- *Most of the IIDTRC incidents were detected by customer complaints, information systems audit and colleagues.*

Perpetrators are not necessarily technical oriented to carry out IIDTRC: This characteristic of the IIDTRC perpetrators suggests that the seemingly least-threatening employees – the call centres employees without technical knowledge or privileged access to retail information systems can still cause significant damage. In particular, the case of 'Jane' (See Section 6.3: Case #1 Personal Identity Theft Related Crimes in the Private Domain: Account Takeover) who stole numerous Credit Card that was left by customers in a rush after shopping. She might not have the technical capabilities of the software engineers, but she used her call-centre skills to use the stolen cards to make purchases from her own company's online portal.

This finding reinforces the recommendation of the role-based framework that retail companies need to adhere to good security principles across all the levels of employees irrespective of their job roles. Hence, this study recommends that companies guide their policies and practices by restricting all levels of employees' access control. In addition, retail companies should assume that potential IIDTRC perpetrator will leverage exploitable IS security vulnerabilities within the research of most non-technical employees (Fichtman, 2001). And there is no amount of IIDTRC prevention systems will defend against such perpetrator. Therefore, online retail companies can only begin to minimise cases of IIDTRC if it continually strengthens their policies on the principle of trusted information systems security and access control mechanisms.

The nature of IIDTRC perpetrated by managers is comparatively different from IIDTRC by shop floor employees: Though the business activities and access to information systems by managers and shop floor employees may have differed at times, managers caused the damages in relation to IIDTRC and evaded being detected for longest amount of time. This finding is evidenced by the case of Jessica Harper; the head of the Lloyds Banking Group's Online Security (see the case #1 of Appendix 3).

In addition, this characteristic suggests the employees of certain job roles such as accountancy and software engineers pose different threats different from the employees at the call centres position. It behoves the companies to consider auditing the activities of employees in relation to features of their job roles. It is essential for e-business companies including financial organisations to develop policies and clearly enforce them to the entire employee with respect to their job roles and business operation but with equal disciplinary actions.

Therefore, a corollary to this varying nature of IIDTRC perpetrators is that practice should be put in place in the companies to disallow regular exception handling or the case of 'different rules for different employees'. In addition, companies should greatly limit the amount of trust they give to employees at the management level. There should be granular access control that is effective enough to provide only necessary access to the employees in management positions. This study, based on the archival analysis findings, suggests that employees in the management position were not closely examined or monitored by the victim companies until it is too late. There should no case of 'sacred cow'; no employee should monitored with preference because of their management position or because an employee makes more money to the company than the other employees.

Some of the IIDTRC incidents were detected through customer complaints, information systems audit and colleagues: The case examples indicate that technology played a very small role in enabling the victim companies to detect IIDTRC. However, by itself this conclusion could be explained by other factors. Perhaps technological approach was largely successful at detecting IIDTRC before more damage was done therefore reducing the impact of the crimes. Additionally, even if the technologically based security systems had been in place, it could be that the systems were out-dated or perhaps have not been installed properly. In the nine case examples discussed in Section 6.3, the victim companies were much successful at detecting IIDTRC by conducting audits, monitoring the employees' suspicious behaviour and questioning the employees' abnormal activities.

Retail companies should establish an anonymous and open communication channel to encourage their employees to report suspicious colleagues carrying out IIDTRC. There should be frequent impromptu and routine information security audit in place to review the operational activities of all employees. There should be a 'no exception rule' no matter the position of the employee in implementing the checks and audit processes.

7.4 Review and Discussion of the Research Propositions

Four propositions were formulated for this study. For all the four propositions, the predicted role-based framework attributes are;

Proposition 1: *Organisations with greater collaboration of management roles are more likely to have effective implementation of IS security strategies required for the prevention of IIDTRC; Management with greater interaction implementing data security roles are likely to achieve organisational goal on IIDTRC prevention;*

Proposition 2: *The greater the inter-dependency of management in carrying out IIDTRC prevention roles, the greater the efficiency in IIDTRC prevention. A collaborative relationship between the management and employees is likely to improve the employees' compliance with Information Systems security policies. The collaborative relationship is likely to improve the effectives of internal data security by directing attention to the IIDTRC risks;*

Proposition 3: *Organisations with greater integration of the management are more likely to have effective collaboration between management roles (IS/T and crime prevention team) in prevention of IIDTRC;*

Proposition 4: *Management with shared understanding of data security operations are more likely to achieve better security strategy in the prevention of IIDTRC. Management role sharing is likely to affect the level of performance management in preventing IIDTRC.Clearly defining the scope of purpose of IIDTRC prevention practices is likely to result in more collaboration and improve performance by the IS security management roles;*

In this current study, these propositions are grouped under the heading 'collaborative management roles for IIDTRC prevention'. Each of the propositions was analysed from perspectives of different attributes of role-based framework by contrasting independent/individual management roles with collaborative management roles.

In addition, the analysis was extended to the influence of role-based framework on the resource efficiency, IS security enhancement and IS security management support.

Proposition 1: Organisations with greater collaboration of management roles are more likely to have effective implementation of IS security strategies required for the prevention of IIDTRC;

Discussions and Implications

This is one of the key attributes of RBF which conceptualises the collaboration of management for implementation of data security practices for prevention of IIDTRC. Online retail companies often neglected collaborative attributes in implementing these practices across their operations, as well as process and technologies. The finding from the *RetailGroup* suggests that the management take sharing of the IIDTRC prevention practices for granted. They handle IIDTRC prevention in relatively independent and predictable ways across their operations while implementing their roles. In particular, the case of *Xtail* suggests that it is vital for the security management their roles and practices within the operational environment. Evidences by the *Ytail* and *Ztail* show that companies that neglect utilising IS management collaborative capabilities usually encounter the challenges identified in *RetailGroup*.

One of the implications of the lack of collaboration in implementing the IIDTRC prevention practices is the issue of misunderstanding in the interpretation of IT security terms. The effect of this misunderstanding can lead to a breakdown and management override. This issue was observed in *Ztail* where the internal auditor was protective and shifting the responsibility to the company's top management. For instance *Ztail*, the internal auditor could not resolve issues related to the IS priority areas; instead he left the responsibility to the head of management. The observation recorded in companies *Ytail* and *Ztail* shows a complete breakdown in communication among the audit team.

These observations provided insights to PWC' ISBS report that 56 per cent of business managers do not work together with their information security auditors. Instead, they leave the responsibility to the information security auditors or rather rely on the contingency plans, with the sole intentions to cut cost or invest less in IT security maintenance. This issue was also noted by Potter and Waterfall (2012) that less than half of the large companies and only a quarter of small ones are collaboratively measuring the coordination of their regulatory data compliance and security management.

Moreover, this issue of perception of ISA costs corresponds to the suggestions of Chris Porter of PWC ISBS (2012) that most managers often fail to evaluate their ISA investment.

Based on the perception of the operation manager of *Ytail* that the approach of the first party audit seems to pay-off by hiring the external auditor, but apparently, the cost of the expended time for the audit and poor audit execution outweigh the benefits of the approach. The operation manager failed to evaluate the pros and cons of paying for the external IS security auditor. This observation confirms Cilli (2003) suggestions that IS management of online retail fail to provide answers to ISA effectiveness and efficiency related questions such as IS security awareness, control and profiling; and performance measurement.

According to the Nieminski (2008), the effective internal control management equips the ISA team to be detective, corrective and preventive to the IIDTRC threats. She further suggested that any crack in the internal control management of the ISA team often lead to limited judgement, breakdowns, management override.

Another notable implication of lack of collaboration of management in implementing effective IIDTRC prevention practices is that companies are likely to develop data security practices that align with the IIDTRC prevention challenges they face. Since such practices lead to a perception of improved IS security, the management may begin to take the challenges for granted. This perception would lead to the development of culturally unethical security practices among the management. Consequently, it then leads to development of internalised IIDTRC prevention practices that are difficult to change. For instance, in both *Ytail* and *Ztail* they relied on the independent ISA from the outsourcing companies. This finding suggested the perception that paying for the ISA checks to the external bodies is enough for effective internal data security. This is observed from the statement made by the operation manager that due to the fact their *Ytail* has paid for the audit, the external auditor bears the whole internal IS security responsibility. This perception contributed to the poor performance of the auditee *Ytail*.

This is because there was no shared responsibility of ISA procedures within the management. The external auditor worked with the available IS resources and information at the disposal to justify the cost of the services being paid for. This observation agrees with suggestions of ACFE (2012) and ISBS (2012) that perception of the high cost of data compliance management and that adequate security checks are already in place often contributes to defectives in the internal data security of most online retail companies.

In order for crimes prevention managers to deliver and counter this challenge of culturally oriented unethical security practices, Innes (2004) suggests that the crimes prevention managers must be integrated into ethical occupational and organisational culture. This suggestion reaffirms the proposition of the Role-based framework that effective integration of cross-functional management team can enhance the management performance in preventing IIDTRC. In order to support the integration and execute the roles of their work efficiently, this suggestion requires that management will endorse the ethical cultural attitudes, beliefs and values to which they are exposed. In other words, the management will have to construct ethical cultural meanings that reflect their occupational responsibilities that are compliant to IIDTRC prevention practices.

However, this proposition of a commitment to IIDTRC prevention might not work for all cases. The strict compliance with the rules of security may encourage managers not to believe in themselves or not following their instinct in managing IIDTRC cases they considered as a suspicious activity.

An attempt to abide by strict compliance rules may develop a perception of which managers conceive as shared understanding of avoiding the potential for deviation from security compliance rules and to avoid scrutiny from their top managers. The shared understanding between the security managers would be focused on their occupational goal of 'getting the job done', avoid criticism from the top managers by sticking to the clear security rules of the shared culture. This perception is what Van Maanen (1974) calls 'cover your ass; characteristic of the security culture; which means "good story maxim". That is, the security managers would make a conceivable story to cover them for everything they do while on their duty in the name of abiding by culturally oriented security practices and security compliance rules.

Conclusions and Recommendations

The discussion of how the cultural orientation of management impacts the practices of IIDTRC prevention in the *RetailGroup* and by drawing from suggestions of previous studies on how this issue affect crimes preventions in crimes' general sense indicates that there is strong need for change in retail companies' security strategy (to included clearly defined ethically security practices).

Importantly, the major change should be the review of the existing security culture, policies, procedures, structures and systems.

Previous studies (e.g. McDonald and Nijhof, 1999; Roukis, 2006; Sekerka and Bagozzi, 2007) argue that implementing an effective ethics programme in an organisation would make the management and employees aware of formal organisational goals, IIDTRC prevention goal in this case, and their informal norms.

Pelletier and Bligh (2006) recommends that business organisations should have a suitable procedures and systems for ethical decision-making regarding their employees roles and responsibilities. This suggestion which corresponds with the suggestion of this research asserts that establishing and putting emphasis procedures and systems would enhance necessary skills for ethical practices in the retail companies.

Moreover, there is the need for retail companies to invest in collaborative management approach in the prevention of the IIDTRC. This practice can improve the overall IS security effectiveness and reduce the impact of the identified challenges of preventing IIDTRC in the online retail companies. Additional benefit may accrue from these practices when supplemented with collaborative ISA by the management. However, the benefits might depend on the level of IT skills of the management, the perception of the management roles, top management support and the organisational operations. The findings from the cases (*Xtail*, *Ytail* and *Ztail*) confirmed that collaborative roles sharing attributes of RBF would enhance the likelihood of effective and strategic prevention of IIDTRC in online retail. It suggests that collaborated approach where internal and external audit work together is a more robust audit practice than first/second party audit that entail either an internal or external auditor.

The collaborative approach is more effective in putting a check on the internal control of IS in a company. This practice would enable the data security audit team to stay abreast of the evolving IIDTRC. It would improve sustainable internal control management through an effective collaboration of essential IS/IT skills in the ISA team. The collaborative functions between IS auditor and IS/IT support encourages two-way communication which is vital for keeping a spotlight on any potential IIDTRC risks. It will encourage online retail managers to hire and incorporate the skilled IS/IT professional in ISA team. It will also enhance the management capability to counter the trending cases of IIDTRC resulting from increasing migration of businesses into the digital realm.

Proposition 2: The greater the interdependency of management in carrying out IIDTRC prevention roles, the greater the efficiency in IIDTRC prevention. A collaborative relationship between the management and employees is likely to improve the employees compliance with IS security policies. The collaborative relationship is likely to improve the effectiveness of internal data security by directing attention to the IIDTRC risks and minimize the challenges encountered by the management;

Discussion and Implication

Based on the discussions above, the impact of the IIDTRC prevention challenges that are encountered by IS security and crime prevention management can be minimised by effective management interaction. This key attribute of the RBF suggests that management interaction can positively impact the management performance by minimising the impact of the challenges (e.g. lack of clarity of roles, lack of management support, segregated authority, and operational changes) encountered by the management on IIDTRC prevention. These identified challenges are suggested to the consequences of lack of interaction between management roles. Each management (or complementary group) works independently to its data security roles. Management often sticks to their roles and practices as they are used to working in their operational environments. If there is no management interaction, conflicts beg the question of which IIDTRC prevention practice to follow. Reconciling these differences and resolving how to act in the face of unfamiliar management often lead to extra work and misunderstanding. Hence, the extra cost to data security implementation in terms of money, quality and time. The issue of lack of clarity of roles and lack of management support evidenced from security auditing in *Ytail* and *Ztail* would have been avoided if there was effective interaction of roles across the audit team. The presence of skilled and experienced management could have resolved the clarity of roles and support issues.

As evidenced by the *Xtail*, the collaborative roles sharing could impact the performance in implementing data security tools. Unlike the *Ytail* and *Ztail* where there were independent handling of IIDTRC prevention roles as a result of ignorance on the part of the audit team on how to go by their roles' interaction followed in their roles differences. This suggested the fact that a different role that exists in different online retail operations with different IS capability can be resolved relatively through collaborative role sharing. The two differing perspectives about IIDTRC prevention responsibilities contribute to a setback in the prevention of these crimes.

This uneven clarity of crime prevention strategies and paralleled sharing of roles among the management has led to inefficiency and poor performance in implementing internal data security tools and strategies. This finding confirms the assumption of the organisation role theory that unclear roles and responsibilities of the management may create ambiguity in the prevention of IIDTRC in an organisation.

To tackle this problem, top management has to embark on e-learning test and criminal law course to enlighten employees on the data security policy and IIDTRC prevention awareness. The data compliance and IT security management have also designed auditing routines and used coercive strategy to ensure that the outsourcing firms are abiding by norms of data security policy. The learning approach adopted by the top management agrees with the recommendation of the RBF approach; which explains the impact of clear roles and responsibilities across all the actors involved in prevention of IIDTRC in the online retail. In their work, Han, Kauffman and Nault (2011) and Zhang, Agarwal, and Lucas, (2011) also noted that investing in training of management and employees have a positive and economically meaningful contribution to industry towards achieving business objectives.

Conclusions and Recommendations

These findings suggest that collaborative audit approach is a more robust practice in detecting IIDTRC risks and their preventions. In addition these findings suggest that an effective collaboration of the audit team would provide better returns on outputs, cost, quality, resources, and time which neither independent external audit nor internal audit would comparatively provide. This study suggests that engaging in either an independent external audit or internal audit would require more work on the security auditor's part in carrying out internal control management and audit plans accordingly.

Although, ISO 19011: 2011 and ACFE (2012) suggest that there is a chance for external ISA auditors to detect IIDTRC risks, this study suggested that such a chance still depends on the cooperation of auditee management. Similarly, engaging in independent internal audit would do little to meet the expectations of the IS security audit regulatory bodies; as seen in the case of *Ytail*. This suggests that the effective exchange of data security strategies between the external and internal auditing should be paramount in companies that are working together to improve their internal data security.

Proposition 3: Organisations with greater integration of the management are more likely to have an effective collaboration between management roles (IS/T and crime prevention team) in prevention of IIDTRC;

Discussions and Implications

The goal of preventing IIDTRC in online retail depends on how the roles (Security Support, IIDTRC Incident Investigation, Data Compliance Management, IIDTRC Prevention, Security Operation, Technical Security, Software Engineering, and Human Resources) interact with each other. The effectiveness of their interaction can be measured by the extent on how they reduce the impact of their challenges posed by IIDTRC such lack of resources, IIDTRC prevention and data protection policy, IS/T Security complexity, lack of clarity of roles, segregated authority, and operational changes. The evidence from the *RetailGroup* that the management are not well-resourced or do not act in a support capacity.

There were always need for the secondary considerations for capabilities and support capacities and changing of processes from the complementary management such as law enforcement agency. For instance, the Head of crimes investigation noted the difficulty his team faces in trying to build effective working relationship with the management of the local law enforcement agency.

He noted that this issue often led to delays during investigation of crimes;

> "*When there is the change of the head of local area police, all the long built relationship and working team would breakdown…, to build up a relationship with the new administration is not easy! Sometimes it is not easy to find the police officer that would play the role of effective investigation of IIDTRC…it is always problem…it is, yes it is…this always lead to delays of investigation and prosecutions……*"

This statement suggests the challenge of establishing lasting support with the law enforcement agencies and *RetailGroup*. And in the online retail environment like this, this situation often leads to the protracted investigation process, and much damage would be done to *RetailGroup*. The longer the investigation took, the more damage the IIDTRC perpetrators would do with the stolen data/information (Lacey and Cuganesan, 2005).

The implication of these observations is the failure of adequate investigation and remediation measures to IIDTRC incidents subsequently detected.

These observations have the implication on the internal security controls and processes employed by the online retail security management. For instance, the statement made by the head of IT security support of *Xtail* that, "…y*ou don't have to be spending money in every IT programme and chips…they are money……in some cases it doesn't worth investing….";* provided the answer why some companies still fall prey to the IIDTRC, amidst all of the security controls. These occur because of weak internal data control systems and out-dated intrusion prevention controls attributed to cost and lax attitudes of management investing in security resources.

This observation corresponds to the Steinnon (2006) report that some companies fail to identify IIDTRC risks because the security controls are not keeping pace with the evolving technology used by the perpetrators of these crimes; instead, the evolving security threatening technologies make the crimes mechanisms easier.

Conclusions and Recommendations

With the lack of resources, other roles and responsibilities would be affected. The ripples of this challenge would impact how the management learn, learn and react to the IIDTRC incidents. It would also affect how the IS security management implement controls and processes in anticipation of the IIDTRC risks.

The impact of the lack of resources would be huge on the management if there is no support of the internal and external cross-functional management team – IT security, crime prevention and law enforcement agencies, as have seen in the above discussion. These findings suggest the need for the IS security and crime prevention management roles to be mastered by the cooperative effort of the management team. The mastery roles attributed to the RBF requires an effective assurance on the security of the company PII/D assets. Thus, the management would be encouraged to update the security tools and data compliance regulations to reduce evolving IIDTRC risks.

For instance, the collaborative ISA approach adopted by *Xtail* enabled them to build a strong workforce that was shown by their level of integrity and competency in prevention IIDTRC. The audit team of *Xtail* took control of the internal IS security issues which ease the audit activities, reduce the expended audit time and cut down logistics related audit protocols. Hence, collaborated ISA enhances the chance to identify IIDTRC risks. Hooks and Kaplan and Schultz (1994) suggest that IIDTRC risks could be detected and put under control if the organisation and external auditor work together.

If the audit team focused more on internal control, they could easily control the organisation's data environment, improve risk assessment and ISA monitoring and enhance the team's communication. Johnson and Rudesill (2012) agree with this suggestion that business owners, management and data security auditors should share the responsibility of IIDTRC prevention.

There is the need for every unit of the IS management to liaise with each other, prioritise the internal data security and control strategies and be a watch-dog to the business. There should be coordinated approach toward assigning the responsibility of IS security. The crack that was often created due to a split in roles of data security can be corrected by effective integration, coordination and communication with the management, external auditing, IT experts and internal auditing.

Proposition 4: Management with shared understanding of data security operations are more likely to achieve better security strategy in the prevention of IIDTRC. Management collaborative role sharing is likely to affect the level of performance management in preventing IIDTRC. Clearly defining the scope of purpose of IIDTRC prevention practices is likely to result in more collaboration and improve performance by the IS security management roles;

Discussions and Implications

The matrix table of management roles in chapter 6 is not merely to draw attention to the fact that differences exist between cross-functional IS management team – an observation that is quite intuitive for most IS security practitioners. By understanding the issue of IS security management on implementing IIDTRC prevention as resulting from team challenges (e.g. internal policy, is/t staff competence, is/t security complexity, security budgets, is/t security tools), provides a clear understanding of application of rbf in resolving these challenges.

By analysing the challenges the IS security managers face in preventing the IIDTRC, this research provides a robust framework to understand and solve the identified challenges. Understanding the attributes of RBF and how it fit into different business operation can minimise these challenges. This agrees with the suggestion by the researchers (e.g. Homel, 2010; Anderson and Tresidder, 2008) that identifying the IIDTRC prevention challenges can be addressed by understanding the roles of IS security management; as an individual and a team.

Lack of management support between management IS security implementation has been a significant challenge. The cases of *Ytail* and *Ztail* indicated that the issues of segregated data security roles have an impact in the allocation of the available resources. Researchers (Lacey, and Cuganesan, 2005) have noted that these varying and segregated data security issues can weaken implementation of data security strategies by increasing the time for data security implementation as well the cost.

These issues could lead to IT budget related issue which was noted as one of the IIDTRC prevention challenges by the *RetailGroup*. The implication of this finding is that sharing of the roles by *Xtail* provided the opportunity to leverage on their management capability. Thus, improving the performance of the management and resolving the issue of segregation of management and reduction on cost and time.

Conclusions and Recommendations

These observations draw a line between the benefits of RBF and the other IIDTRC prevention frameworks. The collaborative roles sharing attributes of RBF adopted by *Xtail* is suggested to be the robust and more efficient in prevention IIDTRC in online retail. The use of the collaborative role sharing ISA approach by *Xtail* was enhanced by the audit team members aligned with skills contributing immensely to their satisfactory ISA assessment. This finding agrees with suggestions of Steinbart*, et al*., (2012), that the relationship between the IS security auditors affects the quality of the ISA practices. The RBF attribute regarding the collaborative roles sharing audit observed in *Xtail* encourages a reliable audit report, efficiency and effectiveness of the audit operations and compliance with applicable ISA regulations.

This RBF attributes sum up the objectives of ISO 19011:2011 and also defined the processes of effective internal IS security control management. This is consistent with the suggestion by SANS Institute report by Kee (2001) that effective internal IS security control management is a vital tool for reducing online retail's data leakages and IIDTRC risks. It noted that it is the responsibility of the internal audit team to highlight the significant data security risks, identify the flaws in data compliance controls, policies and regulations and presents them to the management. As also suggested by Asare and Wright (2004), effective fraud risk assessments are directly associated with an effective collaboration of the fraud specialists practices. The audit criteria attributed to the robust security audit practice of *Xtail* is their proactive and effective internal IS security control.

7.5 Summary of the Discussions

This research discussion have contributed to the suggestions by researchers (e.g. Wright, 1998; Jamieson *et al.,* 2008) that available IIDTRC prevention have concentrated only on generic framework without paying attention to the specific business context. While some (e.g. Niekerk and Solms, 2010; Bishop and Gates, 2008; Jamieson *et al.*, 2009) concentrated on the soft-based security frameworks, and others (e.g. Currie *et al.,* 1999) on the specific context of the business operational environment of the crimes. In particular, this research has provided sector-based understanding of the issues of IIDTRC prevention. It introduced the notion of integrating process and technology approaches to IIDTRC prevention.
The notion was centred on people, the capacity of IS security management. These three categories, particularly the people-centred security, subsume most concept of the role-based framework. The IS security practitioners can now evaluate their roles capacity on prevention of IIDTRC specific to their business operation. The concept is opposed to broadly evaluating the management roles based on a generic framework or software-based security.

Adopting the concept of RBF in this study lead to redefining the capability of IS security management by examining the workings of a collaborated management roles approach compared to the independent management roles approach in prevention of IIDTRC, action research has enabled the researchers to established practical results. It has availed opportunity for the researchers and business practitioners to engage in action that brings about change and knowledge through learning. This contribution to knowledge has succeeded in shedding light on the workings and practices of both first/second party and joint ISA. It will provide a basis for further research in areas of roles of IS security audit in the prevention of IIDTRC in the online retail. Although, RBF might not be a universally applicable concept, IS security managers in e-businesses can benefit greatly from these insights. For example, as a first step, IS security managers can classify each management roles and match them with responsibilities matrix. This could likely produce better roles alignment within the IS security management team handling IIDTRC prevention issues. The challenges in preventing the IIDTRC can be solved through clear information regarding different responsibilities of the IS security managers. RBF thus provides a model where information systems security practitioners and researchers can understand the root cause of issues on prevention of IIDTRC.

Practitioners can design strategic IIDTRC prevention roles that can minimise of each category of IS security management challenge. This RBF approach counter-argues the over-dependence on software security and one-framework-fits-all approaches for prevention of IIDTRC. These issues could be more difficult to resolve. In addition, the issue of aligning the management with suitable IIDTRC roles to make up the management team is most difficult to resolve. Resolving such issue involves in-depth case studies. This issue was observed in *Xtail* case of participant observation. *Xtail* easily dealt with issues that arose due to ISA roles alignment, but was passive in addressing the IS security budget in relation to updating security tools. Thus, the implication of alignment issues resulted in a greater expense of time and poor ISA audit in both *Ytail* and *Ztail*.

These issues may have a heterogeneous effect across online retail companies, suggesting that some may have utilise the collaborative role sharing in their ISA while others did not. In addition, this research confirms Baskerville and Pries-Heje (1999)'s suggestion that action research provides researchers with highly practical results when rigorous attention is given to theory development. It contributes to the knowledge that qualitative research based on limited cases (*Xtail*, *Ytail*, and *Ztail*) might be generalised to theory, but not by population as sought by survey research.

It agrees with Yin (1989)'s argument that limited-case qualitative research does not seek the same sort of generalisability attributed to the population as done in the survey of quantitative research. It enables the researchers to develop the ideas that generalise the cases under study to theory. As noted by Strauss and Corbin (1990), the findings of the research based on grounded theory approach constitute a theoretical formulation of the reality under investigation, rather than consisting of a set of numbers, or a group of loosely related themes. The case study approach has availed the researcher the idea to develop a theory by repeatedly using cycle of inductive and deductive thought. This cycle is repeated in an effort to *ground* the theory in the data.

The grounded theory approach has been applied in this research to define units of analysis. This approach provided more rigorous approaches to theory development. It avails the researcher the technique for integration of with action research and case studies because they are suitable for holding data collation and theory formulation in a reciprocal relationship (Baskerville and Pries-Heje, 1999). Researchers (Strauss and Corbin, 1990; Glaser and Strauss, 1967) suggested that grounded theory is a 'constant comparative method' that alternated the comparison of theory to reality and the building of the theory.

As this research involves careful collation and analysis of empirical data, it began with an understanding of the nature of prevention of IIDTRC and then grounded based on the extension of the role-based framework (RBF). Using grounded theory in this context, enabled the researcher to first develop the conceptual categories from the empirical data (Frankfort-Nachmias and Nachmias, 1992). It enabled the researcher to clarify and elaborate these categories, and makes new observation through field work. This was applied to develop a theory that is 'grounded' and directly relevant to the IS security strategies for prevention of IIDTRC in online retail companies. From these perspectives, the use of the grounded theory holds a promising potential for conducting practical oriented research in the business information systems research.

7.6 Summary of the Implications

This study has several implications for understanding the practices of identity theft prevention. It identifies the attributes that can enhance effective implementation of IIDTRC prevention practices, which has received little IS research attention. The result shows that RBF explains the impact of integration of management on security implementation towards IIDTRC prevention. For comparison, none of the available the identity theft prevention frameworks studies (e.g. Gates and Jacob, 2008; Currie *et al.,* 1999) explained this pattern. Thus, researchers can apply integrated IS security attribute of RBF in future studies. While the findings of this study are in line with previous suggestions (e.g. Vasiu, 2004; Ji, Smith-Chao and Min, 2008; Gercke *et al*., 2011), they also show some unique relationship that were not tested previously. Although, some IS security researchers (e.g. Cappelli *et al*., 2006; Gercke *et al*., 2011) suggest independent management as an effective practice for the IIDTRC prevention.

Role-based framework (RBF) has differentiated the objective measures of coordination and integrated management context from the dynamic measures of IS security implementation. As a result, it was possible to investigate the likely net impact of integrated coordination of management on implementing IIDTRC prevention practices. Among all the attributes of RBF, the significant influences are effective integration management and efficient collaboration roles. This finding reflects the unique IS security management characteristics of e-businesses in general and the online retail, in particular, which tends to counter the challenges of IIDTRC prevention (Okeke and Shah, 2012).

Hence, the analysis of the application of the RBF in the information systems audit of the three selected retail companies suggests to have a sufficient explanatory potential that reflect the practical characteristics of IS security management essential for prevention IIDTRC beyond online retail.

In terms of empirical results, not all the results found here might applicable to all sectors and regions of the world. It is anticipated that if this study were conducted in other countries in Europe, which share similar online retail operation like UK, the findings might be similar.

In addition, given the proportion of cooperation of companies in the sample, it is not surprising that IS security suggested here will be fully established. These firms have the motivations and resources to invest in innovations that can facilitate both short-term and long-term IS security implementation. Other online companies with approximate size like these would experience similar outcomes. If this study were replicated in American countries, Pacific and Africa, the findings might be different. This is because different countries have different access to online retailing IS infrastructure with difference e-business operation. Online retail, by its nature, is one of the e-businesses that are most vulnerable to internal identity theft-related crimes (IIDTRC). This study has provided answers on the nature of IIDTRC in online retail and development of a framework for the prevention of IIDTRC. The analysis of the archival documents has accounted for these crimes nature. In a bid, for the retail stakeholders to combat these crimes, technology-based software security are commonly used, leaving the contribution of the human elements in security implementation less researched. It shows that integrated IS security approach to prevention of IIDTRC within the online retail sector is at the initial state of maturity. Drawing from the recommended practices of identity theft prevention, a role-based framework is developed and empirically evaluated.

This study shows that RBF attributes effects of integrated IS security management and sharing of data security roles among management. It was indicated that both attributes are perceived to impact the implementation of IIDTRC prevention practices. In terms of the RBF attributes impact on prevention of IIDTRC, this research shows that integration of IS security management and complementary management, perceived collaboration of their roles, and leveraging on their capabilities and expertise can play a role in implementing IIDTRC prevention strategies and practices. As a corollary, this research implies that it is the roles of security and crime prevention management to work with the employees, outsourcing firms and law enforcement agencies.

It behoves the management to train and enforce data security regulations. Although, it is less practicable for the management team to implement the best data security practices by employees' trainings, software security and security compliance/regulatory strategy. Proactive strategy such as vulnerability testing on network and web platform, staff vetting and profiling, and customers' IIDTRC awareness campaign might serve as better strategies.

In summary, this research has a number of implications for academia and business managers. For the academia, this research has the following theoretical implications:

- This research has drawn major characteristics of the IIDTRC perpetrator – Perpetrators are not necessarily technical oriented to carry out IIDTRC; the Nature of IIDTRC perpetrated by Managers is comparatively different from IIDTRC by shop floor Employees and Majority of IIDTRC Incidents were detected through Customer Complaints, Information Systems Audit and Colleagues Suspicions. Further research can be designed to examine these characteristics to identify if there is theoretical basis for explaining them

- This research integrates the concepts of human-centred security with technology and process. Through critical explanation of the management roles while applying organisational role theory in a IS security context, it clarifies the role of collaborative management in establishing effective IIDTRC prevention with can promotes the employees' capabilities in maintaining the availability, confidentiality and integrity of online retail IS infrastructure;

- It has contributed to existing knowledge of organisational roles theory by applying it to analyse management roles in the prevention of IIDTRC. It sheds light on the contribution of management roles that facilitates the implementation of the IS security processes. It has analysed the management roles collaboration using the concept of the RBF. It adds to organisational role theory by building on the on-going discourse of how the business environments and organisation operations affect management performance. Thus, bridges the gap that exists in the domain of organisational roles perspectives in IS security management;

- From the research methodology perspectives, this study contributes to the advancement of the interpretive research in IS security management

This study has provided the research setting for applying an interpretive methodology to link a theory to practical analysis of IS security. It demonstrates that mixed method case studies are valuable to provide insights, and interpret relationships between theoretical attributes and constructs;

- It also confirms Baskerville and Pries-Heje (1999)'s suggestion that participation observation research provides researchers with highly practical results when rigorous attention is given to theory development. It contributes to the knowledge that qualitative research based on limited cases (*Xtail*, *Ytail*, and *Ztail*) might be generalised to theory, but not by a population as sought by survey research. It agrees with Yin (1989)'s argument that limited-case qualitative research does not seek the same sort of generalisability.

For the business managers, this research offers relevant practical implications. The contributions of this study depend on the capability of online retail managers to be able to deploy the role-based framework attributes. The findings of this research suggest areas that managers could find vital in securing the IS infrastructure.

The key areas are collaborative information security audit and employees' training. The areas can be used to guide online retail companies in deploying an effective IS security against IIDTRC. Highlights of other practical implications are as follows;

- The IS security implementation for the prevention of IIDTRC is not primarily one manager's roles and responsibilities. It is more of collaborative and participative processes.

- The archival case examples of the IIDTRC perpetrators have provided a description of variables such as age and sex of perpetrators and department of work/job role. Retail companies can infer the characteristics of the IIDTRC perpetrators describe in this research and compare them to their individual company to determine if or/and why the same perpetrator may or may not depart from what was suggested in this case examples.

- The implementation of security practices in online retail companies is not dependent only on hierarchical structured management but across the management. It is the responsibility of every employee to protect the organisation against IIDTRC and data leakages.

- This research suggests HR and data compliance managers play major roles in the prevention of IIDTRC. Their roles are evidenced by the IIDTRC prevention awareness, recruitment processes, clarification of data security policy, counselling and monitoring of the employees business operations.

- Human-centred security is an integral component of effective internal data security against IIDTRC. Thus, it stands to reason that it pays to invests in end-user development and management roles sharing. These practices can improve the overall effectiveness of online retail companies IS security in preventing IIDTRC. Additional benefit may accrue from these practices when supplemented with collaborative ISA by the management. The benefits depend upon the level of management skills, their perception of their roles, top management support and the organisational operations.

- Integration of all the components of the IS security infrastructure in online retail is imperative for the effective IIDTRC prevention. Thus, equal attention should be given to security technology, the implementation processes and management roles.

- The relevance of clarity of roles across Information Systems security management in the prevention of IIDTRC. This research suggests the importance to enforce of clarity of IS security policy across the employees through training and information security audits. The attributes of RBF are influenced by effective collaboration, communication, enforcement, sharing and reporting of IIDTRC issues.

The next chapter concludes this research by looking at contributions, limitations and general lessons which can be drawn from this research for future research plans.

CHAPTER 8

CONCLUSION

8.1 Introduction

To large extent software security and generic framework for prevention of the Internal Identity Theft Related Crimes (IIDTRC) have been previously developed. These preventions, however, do not provide the appropriate Information Systems (IS) security needed in the online retail. This issue necessitates the relevance of this research to provide a comprehensive IIDTRC prevention framework. This research has recognised the imperative to include roles of management in ensuring the effective prevention of the IIDTRC in online retail. Thus, this research provided a role-based framework (RBF) as a tool for the effective prevention of IIDTRC. It has provided the necessary elements that can optimise the contribution of the IS security management in order to implement IIDTRC prevention practices. Therefore, this research is significant. It has looked into the IS security issues in the context of online retail companies and provided a framework for prevention of IIDTRC.

This research has achieved this aim through the four objectives that were set out in chapter 1. First, it has provided the understanding of the nature of IIDTRC in online retail. This objective was achieved through the contribution of the results from the archival analysis which complements the suggestions provided in the literature review. Second, it has identified an applicable framework for prevention of IIDTRC by extending the application of the role-based framework (RBF). This was done through the case studies analysis on how RBF can be applied by the online retail IS security management. The remainder of this chapter discusses contributions of this research, its limitations and suggestions for future research.

8.2 Research Contribution

The primary contribution of this research is that it has provided an analytical nature of IIDTRC in online retail. And has extended the application of the role-based framework (RBF) to the management in carrying out the responsibilities and practices in the strategic prevention of IIDTRC in online retail. This framework helps to structure the key management roles and practices in the online retail information security management. And emphasised the theoretical implication of these roles based on the organisational role theory.

For the information systems management in online retail to implement effective systems security for prevention of IIDTRC, the strategy of management works in unison with clarity of roles should be adopted to reduce the impact of the challenges that can hinder the IIDTRC prevention framework implementation. This is evidenced by the suggestion that collaborative Information Systems security Audit (ISA) which involves cross-functional crimes prevention team can enhance management performance in achieving the IIDTRC prevention goal.

Since a few online retail companies may have incentives to invest resources in their IT security, using collaborative role sharing approach could minimise the impact of these challenges. And such retail companies may be able to reap the benefits of such investment on the long-term. Software security and coercive data security controls have been the strategies most online retail may adopt. The RBF approach along with coercion and training can enhance long-term as well as immediate effective internal data security and crimes prevention. As a corollary, this research implies that it is the roles and responsibility of top security and crime prevention management who are likely to work with the employees, outsourcing firms and law enforcement agencies, to encourage them to adhere to data security strategies and policies. Thus, it behoves the retail IS security management to prevent IIDTRC by training the employees and enforcing data security policies and regulations.

It is evidence in this research that it is less practicable to expect the management team to easily transfer and share their best data security practices by only trainings and coercive strategy. Proactive actions such as effective staff vetting and profiling, and customers' IIDTRC awareness campaign might also serve as an effective measure to prevent crimes. In addition, a proactive vulnerability test on both the network and web platform might serve as a better practice to prevent IIDTRC loopholes and internal data leakages.

In summary, this research has contributed to the knowledge of the prevention of internal identity theft related crimes (IIDTRC) in online retail. It has shown that in the increasing incidents of IIDTRC in online retail, the strategic collaborative management capability can improve IS security. This research suggests that the use of human-centred security can enhance the IS security efficiency and performance in preventing IIDTRC. By extending the used of the role-based framework (RBF), this research has suggested the benefit of integrating management roles in implementing IS security practices.

Hence, this research contributes to both information systems security management and identity theft prevention research in online retail in the following dimensions;

i. The archival analysis results suggest that IIDTRC incidents are not prevented because the management depends on the technological capabilities of software security. And they neglect the monitoring and security audit capabilities which were revealed to have been used to detect the majority of IIDTRC cases. This suggests that it requires comprehensive IS security management attention for effective IIDTRC prevention practices to be implemented.

ii. The finding of this research contributes to new insights into the sector-based study of identity theft, which has not been delineated by the previous studies. It has distinctly describes the issues that could help the understanding of the complex nature of identity theft related crimes in the retail sector. It has answered the question of what the profile of a typical internal identity theft perpetrator looks like in the retail sector by providing the in-depth case examples.

iii. The IS security implementation inertia that online retail companies face in the revention of IIDTRC vis-à-vis the challenges is reflected in the negative linkage between management independent roles and team roles. Perceived collaboration of roles within the IS security management and complementary management (HR and law enforcements) and support from the top management play a significant role in effective implementation of IIDTRC prevention strategy.

iv. This research presented a conceptual framework by combining organisational role theory and IIDTRC prevention practices to develop a role-based framework (RBF). This framework provides descriptive and practical recommendations for the IIDTRC prevention strategy that have been suggested to reduce employees' tendency to indulge in IIDTRC.

    This contributes new insights into the influence of the IS security and crime prevention management roles in the prevention of IIDTRC. And has provided the theoretical lens that may also be used in other related IS security studies in similar context for deeper understanding of identity theft prevention.

v. Based on the role-based framework (RBF) concept, the clarity of roles, roles sharing and perceived collaboration within the operation of IS security management have been suggested to have impact on the prevention of IIDTRC in online retail companies. Among these attributes, clarity of roles and perceived collaboration have the strongest effect. To some extent, the perceived collaboration of management roles can be a very effective implementation security strategy for the prevention of IIDTRC when mediated through managerial competence and aligned complementary management interaction. A greater degree of perceived collaboration in the prevention of IIDTRC is associated more with interaction and less with managerial competence.

The latter attribute can be leverage through effective sharing of roles and better interaction among IS security management. The perceived collaborative roles among management, as an attribute of RBF, explain the influence of interdependency of management in carrying out IIDTRC prevention roles;

i. In terms of practice, this study has identified that online retail IS security management are posed with various challenges that affect the IIDTRC prevention. However, the effective alignment of expertise, integration of management and collaborative of management roles, plays a great impact in managing the identified challenges.

ii. This study indicates that integration of IS security management has an impact on the collaboration of their roles. It suggests that leveraging on their capabilities and expertise can play a role in implementing IIDTRC prevention strategies and practices. These are important to create a strategic internal security controls which can build resilient IS security.

iii. The relationship effects of the RBF attributes to the implementation of IIDTRC prevention practices indicate a possible relationship between IS security and complementary management influences worth exploring in future studies. Previous studies (e.g. Gates and Jacobs, 2008; Andi, 2009; Bielski, 2008) that recommended management effects on the IIDTRC prevention strategies have not evaluated this possible relationship that might exist between IS security management and complementary management. It offers a new contribution to the field of IS security management and may provide opportunities for further research in identity theft prevention.

Having summarised the contributions of this research, it is importance to show how the research objectives outlined in the formulation of this research have been met. Hence, the outcome of this research in relation to meeting the research objectives is presented in table 42 below.

Research Objectives	Chapters and Sections
Provide understanding of the nature of IIDTRC in online retail.	Chapter 2 and Chapter 6.2
Identify a framework for prevention of IIDTRC in online retail.	Chapter 3
Evaluate the resulting framework to understand how the attributes of the framework impact on online retail companies' IIDTRC prevention practice.	Chapter 4, Chapter 5 and Section 6.3
Examine how the IIDTRC prevention framework can be applied by the online retail IS security management.	Chapter 6 and Chapter 7

Table 42: Research Objectives and their Respective Discussion Chapters

The first objective of this research was met with the completion of chapter 2 and section 6.2 where the nature of IIDTRC in the online retail was studied and analysed. The multi-faceted nature of IIDTRC – the methods of perpetration, case examples of IIDTRC perpetrators, their motivations and how they were detected, were examined and the need for research on this subject was established. The examination of the existing literature in chapter 2 set the requirements for the research.

The second objective refers to the IIDTRC prevention framework identification part of this research. In particular, Chapter 3 provided this identification and extension of the framework that form the role-based framework as the resulting outcome. The third objective covered the evaluation of the role-based framework. The discussions of the approaches that were used the evaluation of the role-based framework and research outcome were presented in the Chapter 4 and chapter 5 respectively. Chapter 5, in particular, presented the results of the empirical research and evaluation outcomes of the research. The discussions of the research outcome, which satisfied the requirements of the fourth objectives, were presented in chapter 7.

In addition, the contributions discussed have provided insights to the research questions set out in chapter 1. The insights are summarised in relation to the research questions as shown in table 43 below.

Research Questions	Research Insights
What is the nature of IIDTRC in online retail?	Explanation of the nature of internal identity theft in online retail. It has provided knowledge of the nature of IIDTRC in online retail. It addressed the methods used by perpetrators in carrying out IIDTRC and provided the analysis of the recommended IIDTRC prevention practices.
What framework can be used to prevent IIDTRC?	Synthesis of the recommended identity theft prevention practices into the role-based framework by defining the attributes of the role-based framework into integrated IS security management construct and identifying and validating elements to apply the attributes. This research has gone beyond the research of software-based security and unravels the important of management roles in the application IIDTRC prevention framework. It uses the concept of role-based framework (RBF) to guide the collaborative sharing of roles across IS security management.
How can online retail companies achieve a practical IIDTRC prevention with respect to the attributes of the resulting IIDTRC framework?	The empirical evidence on the handling of IIDTRC incidents by the IS security and crime prevention management was conducted by qualitative case studies. It used the organisational role theory to analyse and guide every stage of the investigation. It has evaluated the impact of attributes of role-based framework on internal identity theft prevention practices in online retail companies. In addition, it contributes to the knowledge of collaborative IS security management in the prevention of IIDTRC and adding to sector-based attributes of RBF in e-business knowledge of identity theft prevention.

Table 43: Research Question and Research Contributions

8.3 Limitations of the Research

The limitations of this study were seen in the two areas – theoretical and methodological. Theoretically, this study relies primarily on organisational role theory and suggestions of the other literature (criminology, IS security, and psychology). Since the literature might be limited to their beliefs, their suggestions and constructs on the issues of IIDTRC prevention practices may differ since they originate from different domains. Other theoretical constructs may overlap as shown in Role-Based Framework. The possible differing beliefs were not examined in this study. Methodologically, this research used an interpretive approach. The findings and discussions are based on the interpretation of the researcher.

The researcher may introduce bias by favouring data that supports preconceived ideas (Eisenhardt, 1989). As a result, there is possibility that other researchers would not interpret the data in the same way. Thus replicating the data collated in this research would be problematic. In addition, it is possible to question the validity of the findings because of the interview bias. As noted by Easterby-Smith *et al.*, (1991), research participants may introduce their own answers that may lead to bias views of the inquiry under study. This may have resulted to inconsistencies in the responses accrued from the interviews respondents.

The archival analysis is limited to the information contained in retail companies' reports and documents retained in the electronic archive. It could not depict what was said in the meeting were the reports was presented, nor was it possible to interview the authors of the documents about their experience on the nature of IIDTRC in their companies. The archival research design centres only on analysing a series of the nature of IIDTRC in the online retail companies. It did not provide answers to the roles that were taken by the companies' management in preventing IIDTRC. For example, it did not answer questions related to why some IIDTRC were handled by IT security while others were done by the crime prevention, and why some IIDTRC incidents reported while others were not.

The archival analysis based on the reports might not have a fact-finding nature of the IIDTRC in retail companies, but instead addresses issues and practices in handling the incidents of the crimes. There are well-known victimising effects for the companies affected by IIDTRC, and potentially victimising effects of the documented reports linked to such companies; but in the absence of in-depth interviews, the archival analysis cannot determine the actual impact of such victimising effects.

It is possible, however, to draw inferences from the analyses of the nature of IIDTRC and their measures based on the both approaches – archival analysis and interviews. The case studies design has some limitation. It is designed based on relatively small number of cases and participants. This affects the generalisability, reliability and validity of the research findings.

Although, the case-control approach was sought, it is important to recognise that the sample population is small to provide generalizable representative data on the perception of the management.

The scope of this research is limited to mostly key IS/T and crime prevention management such as IT security officers, operational managers, HR managers, and key law enforcement agents. In terms of this sample size, though the focus research was on the population of the management in four selected companies, a larger sample size is desired for a greater external validity of the findings. Future research with larger sample size is therefore needed to test if the findings are replicable. This study has considered the online retail of UK as one example of the retail industry. These limitations imply that findings documented here should be generalized with carefulness.

The findings of this study are not the complete cases but can be the considerable insights into the issues of IIDTRC encountered by the management in online retail companies. While *RetailGroup* case analyses were not extreme, the codes categories summarised above could not be considered complete representative of IIDTRC prevention management issues. In addition, the case selection was restricted to retail companies that share relatively similar business operation and management culture, and, therefore, the findings cannot be overgeneralised to all retail industries.

Although, the cooperation of these companies was great, some of their audit result sheets were not released to the research team. The companies perhaps viewed releasing some of these confidential documents as a security risk and might portray them in an unfavourable light. This limited the interpretation on some investigated security issues. Also, while assurances of anonymity and confidentiality were upheld throughout the research, we would not ignore participants' bias in the interview sessions. These research constraints risk the validity of the findings. Besides, the above limitations threaten the repeatability of this study. Repeatability might be impossible due to its contextual nature.

8.4 Further Research

Nevertheless, both the online retail and single country focus do not lead to suspect that Role-based framework might not be applicable to other industries and countries. Further studies covering other sectors of e-business and several countries would shed light on interesting questions such as;

i. Does the pattern of the RBF attributes identified in online retail prevail in the prevention of IIDTRC in other sectors?

ii. What other relationship exist and how are they different from the attributes those emerged in this study.

RBF attributes described in this study can constitute a guide much further studies. RBF can be applied in further research to identify and evaluate the effectiveness of IIDTRC prevention strategies in e-businesses.

To achieve this aim, the research objectives of the research can be set as follows;

i. A systematic review of literature on the nature of practices of IIDTRC prevention in e-businesses;

ii. Use multi-method approaches with multivariate statistical analysis (e.g SPSS/STATA) to establish the roles of information systems management in implementing internal data security and IIDTRC prevention;

iii. Use Amos 17.0 to analyse the impact of the perception of the roles of data security management and crime prevention reference groups on IIDTRC prevention;

iv. Provide a model for prevention of IIDTRC based on RBF attributes. The research may be carried out as a comparative case study. It will analyse incidents/cases that fit the definition of IIDTRC in selected retail/banking industry and the related prevention strategies.

The incidents/cases will be identified through semi-structured interview, questionnaire, and primary source materials (via Lexis-Nexis databases) such as UK National Staff Dismissal Register, National Fraud Authority (NFA) archive, The Association of Business Crime Partnerships archive; and other secondary source materials such as public reporting, business crime reports, and web resources.

The criteria for the select cases will be based on: IIDTRC occurred in UK businesses (retail/banking). The findings from these cases will be described using system dynamic model which would be discussed with the team of researchers to determine the pattern of IIDTRC incidents/cases and to validate the insights of the findings.

The validation will provide generalised finding with a degree of confidence in understanding the complex nature of IIDTRC prevention on which RBF implementation would be built. RBF can be used as a model for analysing the roles of management in the prevention of IIDTRC, to provide useful insight into the alignment of IS and crimes prevention management to best roles to handle IIDTRC risks.

Finally, RBF would be evaluated to draw the boundary to its applicability so that all the attributes necessary to generate and understand the prevention strategies of IIDTRC are implemented effectively. This evaluation approach will enable the researchers to include/exclude practical constraints – administrative, cultural, operational and policy-related factors. It will also enable the researcher to delineate the assumptions (human resources roles, environmental design, policies, business culture, etc.) made in this current research design.

REFERENCES

Abagnale, F. W. (2007). *Stealing your life: The ultimate identity theft prevention plan*. BroadwayBooks: The Crown Publishing Group, New York.

ACAS, (2008). 'Advisory Handbook: Discipline and Grievances at Work'. Available at:http://www.acas.org.uk/media/pdf/s/o/Acas-Guide-on-discipline-and grievances_at_work _(April_11)-accessible-version-may-2012.pdf, Accessed 7 December 2011.

Acoca, B. (2008). 'Online Identity Theft', *Organisation of Economic Cooperation and Development (OECD) Observer.* **268**, pp. 12-13.

Adams, C. (2008). 'No certainty yet for identity assurance: The need for assuring identity is clear, but the path to achieving it is no'. *Signal,* **63**(1), pp. 83-86.

Ahire, S. L. (1997). 'Total Quality Management interfaces: An integrative framework'. *Journal of Management Science*, **27** (6), pp. 91-105.

Ahuja, V. (1997). *Secure commerce on the Internet.* New York: Academic Press.

Akers, R. L. (2000). *Criminological theories*. Los Angeles: Roxbury.

Akers, R. L., (1990). 'Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken'. *Journal of Criminal Law and Criminology*, **81**(3), pp. 654-656.

Alder, P. A., and Alder, P. (1987). *Membership roles in field research*. Newbury Park, CA:Sage.

Alder, P. A., and Alder, P. (2000). Observational techniques. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 377-392). Thousand Oaks, CA: Sage.

Algozzine, B. and Hancock, D. R. (2006). *Doing case study research: A practical guide for beginning researchers.* New York: Teachers College Press.

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., Stoner, E (1999). 'State of the practice of intrusion detection technologies'. Tech. Rep. CMU/SEI-99-TR-028, Carnegie Mellon University/Software Engineering Institute, pp.1-111.

Anderson J. and Tresidder J. (2008). 'A Review of Western Australian Community Safety and Crime Prevention Planning Process'. Canberra-Australian Institute of Criminology.

Anderson, D. et al, (2005). 'Preliminary System Dynamics Maps of the Insider Cyber-threat Problem'. Group Modelling Workshop at Software Engineering Institute, Carnegie Mellon University, pp. 8-36.

Anderson, K., Durbin, E., and Salinger, M. (2008). 'Identity theft'. *Journal of Economic Perspectives*, **22**(2), pp. 171-192.

Anderson, R. H, et al. (2000). 'Research on Mitigating the Insider Threat to Information Systems'. Proceedings of a Workshop Held in RAND Corporation, Santa Monica, pp. 1-35.

Andi, M. (2009). 'What's Your Fraud IQ?' *Journal of Accountancy*, **207**(5), pp. 1-36.

Andrea, M. M. and E. Rowe. (eds). (2009). *Harbouring Data: Information Security, Law, and the Corporation*. Stanford University Press, Stanford.

Anti-Phishing Working Group (APWG), (2014). 'Phishing Activity Trends Report: Unifying the Global Response to Cybercrime, 1st Quarter, 2014'. Available: http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf, Accessed 10 June 2014.

Arantzamendi, M., Lopez-Dicastillo, O., and García- Vivar, C. (2012). Manual of Qualitative Research for Beginners. Pamplona: Eunate

Ashworth, A. (4th ed)2005. *Sentencing and criminal justice*. Cambridge: Cambridge University Press.

Association of Certified Fraud Examiners (ACFE), (2014). 'Report to the Nations on Occupational Fraud and Abuse: Global Fraud Study'. Available at: http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf, Accessed on 20 April 2014.

Attorney's General Department, (2008). 'Final Report: Identity Crime. Commonwealth of Australia, Canberra'. Available Online at http://www.lawlink.nsw.gov.au/lawlink/SCAG/ llscag.nsf/vwFiles/MCLOC_MCC_Chapterr_3_Identity_Crime_-

_Final_Report__PDF.pdf/ $file/MCLOC_MCC_Chapter_3_Identity_Crime_-_Final_Report_-_PDF.pdf; Accessed on 23 October 2012.

Australian Bureau of Statistics (ABS). (2007). 'Personal Fraud'. ABS Canberra Australian Communications and Media Authority (ACMA).

Ayyagari, R. and Tyks, J. (2012). 'Disaster at a University: A Case Study in Information Security'. *Journal of Information Technology Education: Innovations in Practice*, **11**(2012), pp. 85-96.

Bai, S. and Du, P. (2006). 'An Organization Model based on Party Pattern to Support: Dynamic Change for Role-based Workflow Application'. Proceedings of 2006 IEEE Workshop on Distributed Intelligent Systems – Collective Intelligence and Its Applications (DIS'06), Prague, Czech, pp.337-342. Available at: http://ieeexplore.ieee.org/xpl/article Details.jsp?arnumber=1633465, Accessed on 23 August 2011.

Bamfield, J. (Edition) (2012). 'Shopping and Crime: The Police and Retail Crime', pp.180-192, Palgrave Macmillan.

Band, S. R. et al. (2006). 'Comparing Insider IT sabotage and espionage: A Model based Analysis'. CMU/SEI-2006-TR-026.

Barling, J. (1995). *International Review of Industry and Organisational Psychology*. UK: Wiley.

Baroudi, J. J., and Orlikowski, W. J. (1991). 'Studying Information Technology in Organizations: Research Approaches and Assumptions'. *Information Systems Research,* **2**(1), pp. 1-28.

Basel Committee on Banking Supervision. (2012). 'Internal audit functions in Banks'. Available at: www.bis.org, Accessed 30 September 2012.

Baskerville, R. and Pries-Heje, J. (1999). 'Grounded action research: a method for understanding IT in practice', *Accounting, Management and Information Technology*, **9** (1999), pp. 1–23.

Bavis, C. and Parent, M. (2007). 'Data theft or loss: ten things your lawyer must tell you about handling information'. *Ivey Business Journal Online,* **76** (6), pp.1-9.

Baxter, P., and Jack, S. (2008). 'Qualitative case study methodology: Study design and implementation for novice researchers'. *The Qualitative Report*, **13**(4), pp. 544-559.

Bazeley, P. (2007). Qualitative Data Analysis with Nvivo. London: SAGE Publications.

Berg, B. L. (1998). Qualitative research methods for the social sciences. Boston: Pearson.

Berki, R.N. (Edition) (1986). *Security and Society: Reflections on Law, Order and Politics*. J.M. Dent: London, pp.11-14.

Bernard, H. R. (2006). *Research methods in anthropology*. Lanham, MD: Altamira Press.

Berry, G., Briggs P., Erol, R., and van Staden, L. (2011). 'The effectiveness of partnership working in a crime and disorder context: A rapid evidence assessment'. *Home Office Research Report 52.*

Betz, F. (ed.) (2001). *Executive Strategy: Strategic Management and Information Technology.* Wiley, New York, pp.1-544.

Bhati, A. (2010). 'Quantifying the Specific Deterrent Effects of DNA Databases. Justice Policy Centre'. *The Urban Institute*, pp. 1-59.

Biddle, B. J. (1986). 'Recent Developments in Role Theory'. *Annual Review of Sociology,* 12, pp. 67-92.

Biddle, B. J. and Thomas, E. J. (1979a). Role Theory: Concepts and Research. NY: Krieger.

Biddle, B.J. (1986). 'Recent Developments in Role Theory'. *Annual Review of Sociology*, 12, pp. 67–92

Biegelman, M. T. (ed.) (2009). *Identity Theft Handbook: Detection, Prevention and Security.* New Jersey: John Wiley and Sons, Inc.

Bielski, L. (2005). 'Will you spend to thwart ID Theft?' *ABA Banking Journal,* **97**(4), pp. 54-62.

Bielski, L. (2008). 'Getting IT right by thinking it through'. *ABA Banking Journal.* **100** (7), pp. 43-45.

Bishop, M. and Gates, C. (2008). 'Defining the insider threat', Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead.

Black, D. (1987). 'The elementary forms of conflict management', Lecture Series, School of Justice Studies, Arizona State University, Tempe, Arizona.

Boyle, T. A., Kumar, V., Kumar, U. and De Grosbois, D. (eds). (2007). 'Collaboration in Combating Identity Theft'. Journal of Production and Operations Management, **28** (7).

Bradbury, H. and Reason, P. (2001). *Handbook of Action Research*. Thousand Oaks: Sage.

Braithwaite, J. (1989). *Crime, Shame and Reintegration.* Cambridge: Cambridge University Press.

Bressler, L. and Bressler, M. (2007). 'A Model for Prevention and Detection of Criminal Activity Impacting Small Business'. *Journal of Entrepreneur Executive*,12, pp. 23-36

Bressler, S. M. (2009). 'The Impact of Crime on Business: A Model for Prevention, Detection and Remedy'. *Journal of Management and Marketing Research*, **2**(1), pp.12-20.

Breyer, S. (3rd ed). (2012). 'Reference Manual on Scientific Evidence', The National Academies Press, pp. 1-968. U S: Washington, DC.

British Retail Consortium (BRC), (2011). Retail Crime and Loss Prevention Report, Available at: http://www.brc.org.uk/brc_news_detail.asp?id=2065, Accessed 12 February 2012.

British Retail Consortium (BRC), (2013). 'Retail Crime Survey'. Available at: http://www.brc.org.uk/ePublications/BRC_Retail_Crime_Survey_2013/, Accessed 10/04/2014,

Brooke, C. (2002). 'Critical Perspectives on Information Systems: An Impression of the Research Landscape', *Journal of Information Technology*, pp. 271-283.

Brooks, P. and Kamp J. (1991). 'Perceived organisational climate and employee, Counter-productivity'. *Journal of Business and Psychology*, **5**(4), pp. 447-458.

Bryman A. and Bell E. (2011). (3rd ed). *Business Research Methods*. Oxford: Oxford University Press.

Bryman, A. (2008). (3rd edn). *Social Research Methods*, Oxford: Oxford University Press.

Burke, P. J. (2008). 'Identity Control Theory', In: H., P. Clemens, 'Blackwell Encyclopedia of Sociology', *Reference Reviews*, **22**(3), pp.18 – 18

Burkhalter, C and Crittenden, J. (2010). 'Professional Identity Theft: What is it? Are we contributing to it?' What can we do to stop it?' *Contemporary Issues in Communication Science and Disorders,* 35, pp. 89-94.

Burton, D. (2000). *Research Training for Social Scientists*. Thousand Oaks: Sage.

Butts, J. W. (2006). 'Formal Mitigation Strategies for the Insider Threat: A Security Model and Risk Analysis Framework'. Available at: https://www.afresearch.org/skins/rims/q_mod_be0e99f3-fc56-4ccb-8dfe 670c0822a153/q_act_downloadpaper/q_obj_9390d5ea-5e71-4abb-b3e6-c03c79975762/display.aspx; Accessed 9 October 2012.

Cabri, G., Ferrari, L., Leonardi, L., and Quitadamo, R. (2006). 'Collaboration-Driven Role Suggestion for Agents'. Proceeding of IEEE Workshop on Distributed Intelligent Systems - Collective Intelligence and Its Applications, Prague, Czech.

Cain, M. (1973). *Society and the Policeman's Role*. London: Routledge and Kegan Paul

Calder, A. and Watkins, S. (3rd ed.). (2005). *IT governance: a manager's guide to data security and BS 7799/ISO 17799*. London: Sterling, VA : Kogan Page Limited.

Calvasina, G. E., Calvasina, E. J., and Calvasina, R. V. (2006). 'Preventing employee identity fraud'. *Ethical and Regulatory Issues*, **10**(2), pp. 25-29.

Cameron, K. S., and Quinn, R. E. (1999). *Diagnosing and Changing Organizational Culture.* Reading: Addison-Wesley.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., and Willke, B. J. (2006). 'Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks.' Proceedings of the 24th International System Dynamics Conference. Nijmegen, Netherlands, July 2006.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., and Willke, B. J. (2006). 'System Dynamics Modeling of Computer System Sabotage'. Joint CERT Coordination Center/SEI and CyLab at Carnegie Mellon University Report, Pittsburgh, PA, pp. 1-34.

Carley, K. (1990). *Content analysis: The encyclopaedia of language and linguistics*. Edinburgh: Pergamon Press.

Carson, D. and Gilmore, A. (1996). 'Integrative qualitative methods in a services context'. Marketing Intelligence and Planning, **14**(6), p. 21-26.

Carter, P. (2003). *Managing Offenders, Reducing Crime: A New Approach*. London: Home Office.

Carter, S.M. and Little, M. (2007). 'Justifying knowledge, justifying method, taking action: Epistemologies, methodologies, and methods in qualitative research', Qualitative Health Research, **17**(10), pp. 1316–1328.

Cast, A. (2003). 'Identities and Behaviour'. In: P. Burke, T. Owens, R. Serpe, and P. Thoits (Eds.), *Advances in identity theory and research*. New York, NY: Kluwer.

Chan, Y. (2002). 'Why Haven't we Mastered Alignment? The Importance of the Informal Organization Structure'. *MIS Quarterly*, **1**(2): 97-112.

Charmaz, K. 2000. (2nd edn.). *Grounded Theory: Objectivist and Constructivist Methods*. In: Denzin, N. K. and Lincoln, Y. S. (Eds.), Handbook of Qualitative Research, Thousand Oaks: Sage.

Checkpoint, (2013). 'Security Report'. Available: http://sc1.checkpoint.com/documents /securityreport/files/assets/common/downloads/publication.pdf, Accessed 12 May 2013, pp.4-49.

Chen, H. (1990). *Theory-driven Evaluations*. Newbury Park, CA: Sage.

Chen, P. and Rohatgi, P. (2008). 'IT Security as Risk Management: A Research Perspective'. *IBM Research Report*. Thomas J. Watson Research Centre. Yorktown Heights, NY, USA.

Chen, Y.Y., Shek, D.T. and Bu, F.F. (2011). 'Applications of interpretive and constructionist research methods in adolescent research: Philosophy, principles and examples'. *International Journal of Adolescent Medicine and Health*, **23**(2), pp. 129–139.

Cheney, J. S. (2005). 'Do Definitions Still Matter?' Discussion Paper Payment Cards Centre, Federal Reserve Bank of Philadelphia.

Chia, P. A., Maynard, S. B. and Ruighaver, A. B. (2003). *Understanding Organisational Security Culture*. In: Hunter, M. G, Dhanda, K. K. *Information Systems: The Challenges of Theory and Practice*., Las Vegas, USA: Information Institute; 2003.

Chinchani, R., Iyer, A., Ngo, H.Q. and Upadhyaya, S. (2005). 'Towards a Theory of Insider Threat, Assessment'. Proceedings of the 2005 International Conference on Dependable Systems and Networks, Yokohama, Japan, pp. 108–117.

Cichonski, P. and Millar, T., Grance, T., and Scarfone, K. (2012). 'Computer Security Incident Handling Guide', SP 800-61, Revision. NIST, Available at: http://csrc.nist.gov/publications/nistpubs/800-61 rev2/SP800-61 rev2.pdf; Accessed 27 October 2012.

CIFAS: The UK's Fraud Prevention Service, (2010). 'Staff Fraudscape: Depicting the UK's staff fraud landscape', Available at: http://www.cifas.org.uk/secure/contentPORT/uploads/documentsCIFAS%20Reports/CIFAS_Staff_Fraudscape_May_2010.pdf, Accessed 29 November 2011.

CIFAS: The UK's Fraud Prevention Service, (2011). 'Fraud Trends: Fraud Level Surge Upwards' Available at: http://www.cifas.org.uk/annualfraudtrends-jantwelve, Accessed 26 August 2013.

CIFAS: The UK's Fraud Prevention Service, (2012). 'Staff Fraudscape: Depicting the UK's staff fraud Landscape'.

CIFAS: The UK's Fraud Prevention Service, (2013). 'The True Cost of Insider Fraud, Centre for Counter Fraud Studies', pp. 1-11, Available at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-CIFAS-The-True-Cost-of-Internal-Fraud.pdf; Accessed on 4 January 2014.

Cilli, C. (2003). 'IT Governance: Why a Guideline?' Available at: http://m.isaca.org/Journal/Past-Issues/2003/Volume-3/Documents/jpdf033-ITGovernance-WhyaGuideline.pdf, Accessed on 23 April 2012.

Cilli, C., Carter, C., Fleginsky, S., Hernandez, A., Hector, M. G., MacLeod, A., Niblett, P., Ott, J. G., and Vatsaraman, V. (2003). 'Information Systems Auditing Procedure: Control Risk Self-Assessment (CRSA)'. *Document P5*, pp.1-7.

Clarke, E. (2009). 'How secure is your client data? 5 questions you should ask your IT professionals', *Journal of Financial Planning*, pp. 24-25.

Clarke, R. V. (1980). 'Situational' Crime Prevention: Theory and Practice'. *British Journal of Criminology*, 20, pp. 136-47.

Clarke, R. V. (1999). 'Hot Products: Understanding, Anticipating and Reducing the Demand for Stolen Goods', *Police Research Series*, 98, Home Office, London.

Clarke, R. V. and Harris, P. (1992b.) 'A Rational Choice Perspective on the Target of Auto Theft'. *Criminal Behaviour and Mental Health*, 2, pp. 25-42.

Collins J. M. (2006). *Preventing Identity Theft in Your Business*. John Wiley and Sons Inc. New Jersey: USA, pp.1-256.

Collins, J.M. (2001). 'Preventing identity theft in the workplace using the four-factor model to secure people, processes, proprietary information, and property (virtual and actual)', In: Collins, J. M. and McGinley, T. G. (eds). (2001). Academy of Criminal Justice Sciences 38th Annual Meeting, Identity Fraud Profit and Predictions, Washington, DC, U S.

Collins, J.M. (2003). 'National Institute of Justice Crime Report', U. S. Department of Justice, Office of Justice Programs, Michigan State University, U. S.

Confederation of British Industry (CBI). (2010). 'A Frontline Force: Proposals for More Effective Policing', *CBI Report on Public Services*, pp.1-23.

Confederation of European Security Services (CoESS). (2012). Critical Infrastructure Security and Protection – The Private–Public Opportunity. 2012. Paper and Guidelines by CoESS and Its Working Committee on Critical Infrastructure Protection. May, Belgium.

Consortium for Cybersecurity Action (CCA), (2012). 'Critical Security Controls for Effective Cyber Defence'. Available at: http://www.sans.org/critical-security-controls/; Accessed on 12 June 2012.

Conte, J. M. (2003). 'Cyber Security: Looking Inward Internal threat evaluation'. Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC) paper, practical assignment version 1.4b, pp.1-13.

Cook, T. (1997). 'What is Past is Prologue: A History of Archival Ideas Since 1898, and the Future Paradigm Shift'. *The Journal of Association of Canadian Archivists*, **43**(1997).

Cooper, D. R. and Emory, C. W. (1991) (eds). *Business Research Methods*, Irwin, Boston.

Coote, L. (1994). 'Epistemological foundations of case study research methodology'. Working paper, School of Marketing, Brisbane.

Cornish, D, B. and Clarke, R. V. (2003). 'Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention'. *Crime Prevention Studies*, **16**(2003), pp.41-96.

Cornish, D. (1994). 'The procedural analysis of offending and its relevance for situational prevention'. In: Crime Prevention Studies. In R. Clarke, Ed. Criminal Justice Press, NY, pp.151-196.

Cornish, D. and Clarke, R.V. (1989). 'Crime Specialisation, Crime Displacement and Rational Choice Theory'. In: Criminal Behavior and the Justice System: Psychological Perspective, H. Wegener, F. Losel, and J. Haisch, Eds. Springer-Verlag, NY, pp. 103-117.

Cosgrove, F. M. (2011). An Appreciative Ethnography of PCSOs in a Northern City. Doctoral thesis, Northumbria University.

Crawford, A. (edn). (2002). Crime and Insecurity: The Governance of Safety in Europe. Cullompton: Willan.

Cressey, R. D. (1973). 'Other People's Money: A study in the Social Psychology of Embezzlement', *International Review of Modern Sociology*, **3**(1), pp. 114-116.

Criminal Justice Commission. (1997). *Integrity in the Queensland Police Service: Implementation and Impact of the Fitzgerald Inquiry Reform,* Brisbane: Criminal Justice Commission.

Crotty, M. (1998). *The Foundation of Social Research: Meaning and Perspectives in the Research Process*. London: Sage.

CSO Magazine (2011). 'Most Computer Related Fraud is an Inside Job, Says Survey'. Available at: http://www.csoonline.com/article/693649/most-fraud-is-an-inside-job-says-survey, Accessed 23 September 2011.

Currie, W. C. and B. Galliers (eds). (1999). *Rethinking Management Information Systems: An Interdisciplinary Perspective*. Oxford University Press, Oxford, pp. 1-528.

Dahler-Larsen, P. (1997). 'Moral functionality and organizational identity: a perspective on the new moralized discourses in organizations', *Current Topics in Management*, 2, pp. 305-26.

Danziger, J. N, and Kraemer, K. L. (1991). *Survey Research and Multiple Operationism: The URBIS Project Methodology*. In: Kraemer, K. L. (ed.), *The Information Systems Research Challenge: Survey Research Methods*, Boston: Harvard Business School Press.

Data Protection Act (1998), Part VI (Miscellaneous and General), Section 55, Office of Public Sector Information, Available at: http://www.legislation.gov.uk/ukpga/1998/29/section/4, Accessed 14 January 2014.

Davenport, T., and Short, J. (1990). 'The new industrial engineering: information technology and business process redesign'. *Sloan Management Review*, (Summer), pp. 11–27.

Davis, E. S. (2003). 'A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft via the Internet'. *Journal of Law and Policy*, **12** (1), pp. 201-227.

Davis, G., Hamilton, S. and Ives, B., (1980). 'A framework for research in computer-based management information systems'. *Journal of Management Science*, 26, pp. 910-934.

De Laine, M. (2000). *Fieldwork, participation and practice: Ethics and dilemmas in qualitative research*. London: Sage Publications.

De, K. (2004). 'The Role of Profiling in the Detection and Prevention of Identity Fraud'. University of New South Wales, Australia.

Deacon, D. and Bryman, A. and Fenton, N. (1998). 'Collision or Collusion? A Discussion and Case Study of the Unplanned Triangulation of Quantitative and Qualitative Research Methods'. *International Journal of Social Research Methodology*, **1**(1), pp. 47-63.

Dean, S. et al. (2012). 'Fortifying your defences: The role of internal audit in assuring data security and privacy'. PCW Publications. Available at: http://www.PWC.com/us/en/risk-assurance-services/publications/internal-audit-assuring-data-security-privacy.jhtml, Accessed on 9 October 2012.

Denning, D. E., and William, E. B. (2000). *Hiding crimes in cyberspace*. London: Routledge.

Denzin N.K. and Lincoln Y.S. (eds.) (2011). *The Sage Handbook of Qualitative Research*. London: Sage.

Denzin, N. K. and Lincoln, Y. S. (3rd edn). (2005). *Handbook of Qualitative Research*. Thousand Oaks, Sage Publications.

Denzin, N. K., and Lincoln, Y. S. (2nd edn.). (2000). *Handbook of Qualitative Research,* Thousand Oaks: Sage.

Dewalt, K. M. and Dewalt, B. R. (2002). *Participant observation: A guide for fieldworkers.* New York: Altamira Press.

DeWalt, K. M., DeWalt, B. R., and Wayland, C. B. (1998). *Participant observation.* In: H. R. Bernard (Ed.), *Handbook of methods in cultural anthropology,* pp.259-299. Walnut Creek, CA: AltaMira Press.

Dhamija, R., and Tygar, J. D., and Hearst, M., (2006). 'Why Phishing Works', CHI Proceedings: Security, pp. 581-590.

Dick, D. (2001). 'Action research: action and research'. In: Sankaran S, *et al.*, eds. Effective change management using action learning and action research: concepts, frameworks, processes, applications, Southern Cross University Press, Australia, p. 21-27.

Dick, D. (2002). 'Action research: action and research'. A paper prepared for the seminar "Doing good action research" held at Southern Cross University Press, Australia.

Dion, M. (2008). 'Ethical leadership and crime prevention in the organizational setting', *Journal of Financial Crime,* **15**(3), pp. 308 – 319.

Dittenhofer, M.A., Ramamoorti, S., Ziegenfuss, D.E., and Evans, R.L. (2010). 'Behavioural dimensions of internal auditing: a practical guide to professional relationships in internal auditing'. The Institute of Internal Auditors Research Foundation.

Ditton, J. (1977). *Part-Time Crime: An Ethnography of Fiddling and Pilferage*. London: Macmillan.

Dobb, A. and Webster, C. (2003). 'Sentence Severity and Crime: Accepting the Null Hypotheses', *Crime and Justice,* 30, pp. 143-195.

Dooley, G. (2009). 'The vital nature of registry security'. *Journal Article: Keeping Good Companies,* **61**(9), p. 525.

Douglas, M. (1970). Natural symbols: Explanations in cosmology. Harmsworth: Penguin.

Duffin, M., et al. (2006). 'Identity Theft in the UK: Offender and Victim Perspective'. Perpetuity Research and Consultancy International Ltd, Leicester, UK.

Durkheim, E. (1966). *Suicide,* New York: Free Press.

Earl, M. (ed.) (1988). *Information Management: The Strategic Dimension*. Clarendon Press, Oxford, pp.1-312.

Easterby-Smith, M, Thorpe, R. and Jackson, P. (4th Edition). (2012). *Management research.* Sage, London.

Easterby-Smith, M., Thorpe, R. and Lowe, A. (2nd Edition). (2002), *Management Research: An Introduction*, Sage Publications, London.

Eisenhardt, K. (1989). 'Building Theories from Case Study Research'. *Academy of Management Review*, **14**(4), p. 532-550.

Ekblom, P. (1992). *Preventing Post Office Robberies in London: Effects and Side Effects.* In: R.V. Clarke (ed.), *Situational Crime Prevention: Successful Case Studies*. Albany, NY: Harrow and Heston.

Ekblom, P. (1994). 'Proximal circumstances: a mechanism-based classification of crime prevention', *Crime Prevention Studies*, 2, pp. 185-232.

Ekblom, P. (2010). *Crime Prevention, Security and Community Safety with the 5Is Framework*. Basingstoke: Palgrave Macmillan.

Ekblom, P. and and Pease, K. (1995). 'Evaluating Crime Prevention', In: M. Tonry and D.P. Farrington (eds.), 'Building a Safer Society: Strategic Approaches to Crime and Justice'. Crime and Justice: A Review of Research, 19, Chicago, IL: University of Chicago Press.

Ekblom, P. and N. Tilley (2000). 'Going Equipped. Criminology, Situational Crime Prevention and the Resourceful Offender'. *British Journal of Criminology*, 40, p. 376-398.

Elliot, J. (1976). *A General Theory of Bureaucracy*. Heinemann Press, London, UK.

Elliot, R. K and Willingham, J. J. (eds.). (2001). 'Management Fraud: Detection and Deterrence'. In: Johnson, G. G., and Rudesill, C. L. (2004). 'An investigation into fraud prevention and detection of small businesses in the US: responsibilities of auditors, managers, and business owners'. *Accounting Forum*, **25** (1), p. 56-76.

Elo, S. and Kyngas, H. (2008). The qualitative content analysis process. *Journal of Advance Nursing,* **62** (1), 107-115

Emerson, R. M., Fretz, R. I. and Shaw, L. L. (2001). 'Participant Observation and Fieldnotes'.In: Paul Atkinson, Amanda Coffey, Sara Delamont, John Lofland, and Lyn Lofland (Eds.), *Handbook of Ethnography*. pp: 356-357. Thousand Oaks, CA: Sage Publications.

Endicott-Popovski, B. and Lockwood, D. L. (2006). 'A Social Engineering Project in a Computer Security Course'. *Academy of Information and Management Sciences Journal*, **9**(1), pp. 37-44.

Engel, R. S., Calnon, J. M. and Bernard, T. J. (2002). Theory and racial profiling: Shortcomings and future directions in research. Justice Quarterly, 19, pp. 249-273.

Engel, R.S., Calnon, J.M. and Bernard, T. J. (2002), 'Theory and racial profiling: shortcomings and future directions in research', *Justice Quarterly*, **19**(2), pp. 249-73.

English, B, J. and Cummings, R. and Straton, R, G. (2002). 'Choosing an Evaluation Model for Community Crime Prevention Programmes', *Crime Prevention Studies*, 14, pp. 119-169.

Farrington, D. P. and Petrosino, A. (2000). 'Systematic reviews of criminological interventions: The Campbell Collaboration Crime and Justice Group'. *International Annals of Criminology*, **38** (2001), p. 49-66.

Fay, B. (1996). *Contemporary Philosophy of Social Science*, Blackwell, Oxford.

Fichtman, P. (2001). 'Preventing Credit Card Fraud and Identity Theft: A Primer for Online Merchants'. *Information Systems Security*. **10**(5).

Fichtman, P. (2001). Preventing Credit Card Fraud and Identity Theft: A Primer for Online Merchants. *Information Systems Security*, **10**(5).

Fighting Retail Crime Report, (2012). Available at: http://www.adderdigitalcc.tv/ downloads /EmployeeTheft.pdf, Accessed on 20 April 2013.

Financial Crime and Service Authority (FCSA). (2009). 'Consumer Financial Education: Money Made Clear'.

Financial Insights. (2004). 'Sharing the Best IT Practices in the Finance Sector', IDC/Financial Insights Banking Technology Road show CEE, Warsaw, Poland.

Fitzgerald, T. (2007). *Building Management Commitment through Security Councils, or Security Council Critical Success Factors*. In H. F. Tipton (Ed.), *Information Security Management Handbook*, pp. 105-121. Hoboken: Auerbach Publications.

Flanagan, R. (2008). 'The Review of Policing', *Final Report*, pp. 1-5.

Forrester and Seeburger. (2013). 'The future of Data Security and Privacy: Controlling Big Data', In: the WebCast, 'The Silent Enemy: Preventing Data Breaches from Insiders', 13 March 2013 at 13:00–14:00 EDT.

Forrsights Report (2013). 'Workforce Employee Survey', Available at http://www.freemovealliance.com/wp-content/uploads/2013/06/Orange-Enterprise-Mobililty.pdf , Accessed 1 October 2013

Foster, M. E. (1991). 'Qualitative investigations into schools and schooling'. *Readings on Equal Education*, 11, p. 312.

Frankfort-Nachmias, C. and Nachmias, D. (4th edition). (1992). *Research methods in the social sciences*, London: Edward Arnold.

Fraud Watch (2013). 'Data theft is biggest insider fraud threat', Available at: http://www.fraudwatchonline.com/index.php/news/employee; Accessed on: 3 June 2013.

FraudTrack (2012). 'FraudTrack 9: Under Starters Order'. Available: http://www.ibe.org.uk/userimages/bdofraudtrack9.pdf Accessed on 12 December 2013.

Gabriel, C. (1990). 'The validity of qualitative market research'. *Journal of the Market Research Society,* **32**(4), pp. 507-519.

Galliers, R. (1990). 'Choosing appropriate information systems research methodologies: an updated taxonomy' In: Nissen, H. E. and Klein, H. K. and Hirschheim, R. A. 'Information systems research: Contemporary approaches and emergent traditions'. Amsterdam: North-Holland.

Galliers, R., and Land, F. (1987). 'Choosing appropriate information systems research methodologies'. *Communications of the ACM*, 30, pp. 900–902.

Gambin, L., Hogarth, T., Atfield, G., Li, Y., Breuer, Z. and Richard, G. (2012). 'Sector Skills Insights: Retail. UK Commission for Employment and Skills and University of Warwick Institute of Employment Research'. *Joint Research Report*, pp.1-89.

Gates, T. and Jacob, K. (2008). 'Payments Fraud: Perception versus Reality – A conference summary'. *Journal of Economic Perspectives*, **33**(1), p. 7-13.

Gaudin, S. (2002). 'Social engineering: the human side of hacking'. Available at http://www.cioupdate.com/reports/article.php/1040881/Social-Engineering-The-Human-Side-Of-Hacking.htm, Accessed 12 July 2012.

Gayer, J. (2003). 'Policing Privacy: Law Enforcement's Response to Identity Theft'. Californian Public Interest Research Group.

Gercke, M., de Almeida, G. M., Lawson, P., Callanan, C. and Simion, R. (2011). (3rd edn.). *Handbook on Identity Theft Related Crimes,* United Nations Office on Drugs and Crimes: Publishing and Library Section, pp. 107-169.

Gerring, J. (2001). *Social Science Methodology: A Critical Framework.* Cambridge University Press.

Gibbs, G. (2002). *Qualitative Data Analysis: Explorations with NVivo*. Maidenhead: Open University Press.

Gibbs, J. P. (1968). 'Crime, punishment and deterrence. South-western'. *Social Science Quarterly,* 48, pp. 515–530

Gill, M. (2011). 'Fraud and Recessions: Views from Fraudsters and Fraud Managers'. *International Journal of Law, Crime and Justice*, **39**(3), pp. 204-214.

Gill, M. and Binder, R. (2005). 'Identity Theft and Fraud: Learning From the USA'. Perpetuity Research and Consultancy International Ltd.

Gilling. D. (1993). Crime Prevention Discourses and the Multi-Agency Approach. *International Journal of the Sociology of Law*, **21**(1), p. 145-157.

Gladstone, F. (1980). Co-ordinating crime prevention efforts. London, UK: Her Majesty's Stationery Office.

Glaser, B. and Strauss, A. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research. Chicago: Aldine Publishing Company.

Glaser, B. G. (1978). *Theoretical Sensitivity*. Sociology, Press, Mill Valley, USA.

Glaser, B. G. (2001). *The Grounded Theory Perspective: conceptualisation contrasted with description*. Sociology Press, Mill Valley, USA.

Goffman, E. (1990). *Stigma: Notes on the management of spoiled identity.* London: Penguin.

Gold, R. L. (1959). 'Roles in Sociological Field Observations'. *Social Forces*, 36(3), pp. 217-223.

Gold, R. L. (1969). *Roles in sociological field observations*. In: Issues in participant observation, edited by G. J. McCall and J. L. Simmons, 30–39. Reading, MA: Addison-Wesley.

Golden, L. (2002). *Evaluation of the Efficacy of a Cognitive Behavioural Program for Offenders on Probation: Thinking for a Change*. USA: Dallas, University of Texas.

Goodman, W. (2010). 'Cyber Deterrence: Tougher in Theory than in Practice'. *Strategic Studies Quarterly,* **4**(3), p.103

Gottfredson, S. and Taylor, R. B. (1986). *Environmental design, crime and prevention: An examination of community dynamics.* In: Tory, M and Reiss, A. J. (eds.) *Communities and Crime,* pp. 387-416. University of Chicago Press, Chicago.

Gray, D. E. (2nd Edn). (2009). *Doing Research in the Real World: Theoretical Perspective and Research Methodologies,* Sage: London, pp. 16-38.

Greenberg, L. and Barling. (1996). 'Employee Theft'. *Journal of Organisational Behaviour*, pp. 46-64.

Green-King, T. (2011). 'Social engineering hits 42% Businesses in UK'. Available at: http://www.spamfighter.com/News-16838-Social-Engineering-Hit-42-Businesses-in UK.htm; Accessed on 30 September 2012.

Greitzer, F. L. et al. (2008). 'Combating the Insider Cyber Threat'. IEEE Security and Privacy, **6**(1), pp. 61-64.

Guba, E. G. (1990). *The Paradigm Dialogue*. Newbury Park, CA: Sage.

Guba, E.G, and Lincoln, Y.S. (1985). *Naturalistic Inquiry*. Newbury Park, CA: Sage

Guba, E.G. and Lincoln, Y.S. (1994). *Competing paradigms in qualitative research*. In: Denzin and Lincoln (eds.), *Handbook of Qualitative Research,* Sage: Thousand Oaks.

H M Cabinet Office, (2002). *Identity Fraud: A study*. London.

Ha, D. et al. (2007). 'Insider threat analysis using information-centric modelling', *International Federation for Information Processing*, **242** (2007), pp. 55-73.

Hadfield, L. (2010). 'Balancing on the edge of the archive: the researcher's role in collecting and preparing data for deposit'. In: Shirani, F. and Weller, S. (eds) 'Conducting qualitative longitudinal research: fieldwork experiences', Timescapes Working Paper 2, Available at http://www.timescapes.leeds.ac.uk/events-dissemination/publications.php, Accessed 23 September 2012.

Hakim, C. (1994). Strategic and Choices in Design of Research. New York: Routledge.

Hakim, C. (2nd edn). (2000). *Research Design: Successful Designs for Social and Economic Research,* London: Routledge.

Haley, C. (2013). 'A Theory of Cyber Deterrence', *Georgetown Journal of International Affairs,* Available Online at: Http://Journal.Georgetown.Edu/A-Theory-Of-Cyber-Deterrence-Christopher-Haley, Accessed on 23 April 2014.

Hammersley, M. and Atkinson, P. (2007*). Ethnography: Principles in practic* (3rd edn.). Taylor and Francis e-Library.

Hastings, G., and Marcus, R. (2006). *Identity Theft Inc: A wild ride with the world's number one identity thief.* New York: Disinformation Company.

Hatt, G. (1985). *Method of Social Research.* Mc. Grow Hill Book Co., Tokyo, Japan.

Hinds, J. (2007). 'Tackling Staff Fraud and Dishonesty: Managing and Mitigating the Risks'. Chartered Institute of Personnel and Development Guide, UK.

Hirsch, A. Bottoms, A., Burney, E. and Wikstrom, P. O. (1999). *Criminal Deterrence and Sentence Severity: An Analysis of Recent Research*, Oxford: Hart Publishing

Hirschheim, R. and Klein, H. K. and Lyytinen, K. (1996). 'Exploring the intellectual structures of information systems development: A social action theoretic analysis'. *Journal of Accounting, Management and Information Technology*, **6**(1/2), pp. 1-64.

Hirschman, E. C. (1986). 'Humanistic inquiry in marketing research: philosophy, method, and criteria'. *Journal of Marketing Research*, 23, pp. 237-249.

Hodgson, G.M. (2006). 'What are Institutions?' *Journal of Economic Issues,* **40**(1), pp. 1-20.

Hofmeyr, S.A., Forrest, S., Somayaji, A. (1998). 'Intrusion detection using sequences of systems calls'. *Journal of Computer Security*, **6**(3), pp.151–180.

Hollinger, R. D. (1997). *Crime, deviance and the computer*. Aldershot: Dartmouth.

Holt, C. and Fawcett, S. and Rabinowitz, P. (2012). 'Collecting and Using Archival Data'. Workshop Group for Community Health and Development, University of Kansas, US.

Home Office Identity Fraud Steering Committee. (2006). Updated estimate of cost of identity fraud to UK economy. Available at: http://www.identitytheft.org.uk/ID%20fraud%20table.pdf> Accessed 14 July 2013.

Home Office. (2011a). *A New Approach to Crimes,* Policy Report, In: Policy Report - Helping the police fight crime more effectively, pp. 3-12.

Homel P, (2010). 'Delivering effective local crime prevention: Why understanding variations in municipal governance arrangements matters'.

Homel, P., Morgan, A., Behm, A., and Makkai, T. (2007). 'The review of the National Community Crime Prevention Programme: Establishing a new strategic direction'. Report to the Attorney General's Department. Canberra: Australian Institute of Criminology.

Hooks, K, L. and Kaplan, S, E. and Schultz J, J. (1994). 'Enhancing Communication to Assist in Fraud Prevention and Detection'. *Journal of Practice and Theory,* **13** (2), pp. 86-113.

Hope, T. and Karstedt, S. (2003). *Towards new social crime prevention*, In: H. Kury and J. Obergfell-Fuchs (eds), *Crime Prevention: New Approaches*, Weisse Ring Verlag-GmbH, Mainz, Deutschland, pp. 461-489.

Hosein, G. (2008). *Politics and identity management*, In: Leeuw, E., and Fischer-Hübner, S. and Tseng, J. and Borking, J. (eds). *Policies and research in identity management*, pp.3-4. New York: Springer.

Hough, M. and Mayhew, P. (1983). 'The British Crime Survey: first report', *Home Office Research Study 76*. London: HMSO.

Hsieh, H. F. and Shannon, S.E. (2005). 'Three approaches to qualitative content analysis'. *Qualitative Health Research*, **15**(9), pp. 1277-1288.

Hua, J, and Bapna, S. (2012). 'The economic impact of cyber terrorism'. *Journal of Strategic Information Systems*, pp. 1-12.

Hub International, (2010). 'Identity Theft in the Information Age: Protecting your Most Valued Asset'. White Paper, pp. 1-12.

Huberman, A. M., and Miles, M. B. (2nd edn.). (1994). *Qualitative data analysis: An Expanded Sourcebook of New Methods,* Thousand Oaks: Sage.

Hunter, R., and Ray, J. C. (1997). *Preventing convenience store robbery through environmental design*. In: R. Clarke, Ed. *Situational Crime Prevention: Successful Case Studies*, (2nd edn.) Harrow and Heston, NY.

Hurst, P. (2010). 'Staff Fraudscape: Depicting the United Kingdom's Staff Fraud Land Scape'. CIFAS, United Kingdom.

IBM Software. (2012). 'Avoiding insider threats to enterprise security: Protect privileged user identities across complex IT environments—even in the cloud'. Thought Leadership White Paper, pp. 1-7.

Identity Theft and Assumption Deterrence Act 1998, Public Law 105–318—OCT. 30, 1998 112 STAT. 3007, Public Law 105–318, 105th Congress. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-105publ318/pdf/PLAW-105publ318.pdf, Accessed on 13 March 2014.

Identity Theft Resource Centre (ITRC). (2003). 'Identity Theft: The Aftermath 2002' Published September 2003.

Identity Theft Resource Centre (ITRC). (2005). 'Identity Theft: The Aftermath 2004' Published September 2005.

Identity Theft Resource Centre (ITRC). (2007). 'Identity Theft: The Aftermath 2006' Published October 2007.

Identity Theft Resource Centre (ITRC). (2008). 'Identity Theft: The Aftermath 2007' Published May 2008.

IdentityForce Report. (2014). Identity Theft Protection with IdentityForce, Available: http://www.asecurelife.com/identity-force/, Accessed 12 July 2014.

Innes, M. (2003) *Understanding Social Control: Deviance, Crime and Social Order*. Buckingham: Open University Press.

Irani, Z. (2002). Information systems evaluation: navigating through the problem domain. *Information and Management*, **40** (2002), pp.11-24.

ISACA. (2010). IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals.

Jabbour, G. and Menasce, D. A. (2009). 'The Insider Threat Security Architecture: A Framework for an Integrated, Inseparable, and Uninterrupted Self-Protection Mechanism', International Conference on Computational Science and Engineering, CSE '09, pp.1616-1620.

Jacob, H, (ed.). (1974). 'The Potential for Reform of Criminal Justice'. *Sage Criminal Justice System Annual Review*, 3. California: Sage.

Jakobsson, M. and Myers, S. (2007). *Phishing and Countermeasures: Understanding the increasing problems of electronic identity theft*. New Jersey: John Wiley and Sons.

James, B. (2006). 'Review of the Legal Status and Rights of Victims of Identity Theft in Australasia', Australasian Centre for Policing Research, Report Series, **142**(2), pp. 1-6.

Jamieson, R J., Winchester, D W., Stephens, G., and Smith, S., (2008). 'Developing a Conceptual Framework for Identity Fraud Profiling'. Proceedings of the 16th European Conference on Information Systems at the J.E. Cairnes Graduate School of Business and Public Policy, National University of Ireland, Galway, Ireland, 9-11 June.

Jamieson, R, J., Winchester, D, W., and Smith, S. (2007). 'Development of a Conceptual Framework for Managing Identity Fraud', Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS-40), IEEE Computer Society, (January 2007), pp. 1-10.

Jamieson, R., Land, L. P, W., Smith, S., Stephens, G., and Winchester, D. (2009). 'Information Security in an Identity Management Lifecycle: Mitigating Identity Crimes'. AMCIS 2009 Proceedings.

Jendly, H, Kam J., Idriss M, and Mulone S., (eds) (2010). 'International report on crime prevention and community safety: Trends and perspectives'. Montreal: International Centre for the Prevention of Crime, pp.118–120.

Ji, S., Smith-Chao, S. and Min, Q. (2008). Systems Plan for Combating Identity Theft – A Theoretical Framework'. *Journal of Service Science and Management*. **2008**(1), pp. 143-152.

Johns, G. (1987). *The great escape. Psychology today*. 21, pp. 30-33.

Jorgensen, D. L. (1989). 'Participant Observation: A Methodology for Human Studies'. *Applied Social Research Methods Series*, 15, pp. 108-115.

Josselson, R. and McAdams, D. and Lieblich, A. (2006). *Introduction.* In McAdams, D. and Josselson, R. and Lieblich, A. (eds.). *Identity and story: Creating self in story.* pp. 3-11. Washington DC: American Psychological Association.

Kaffer, N. (2010). 'Businesses need a plan to guard against ID theft', *Crain's Detroit Business Periodical*, **26**(23), p. 11.

Kahn, R.L and Katz, D. (1978). (2nd ed.). *The social psychology of organizations*. New York: Wiley.

Kantor, S. (1983). 'How to Foil Employee Crime'. *Nation's Business*, (July), pp.38-39.

Kaplan, B, and Duchon, D. (1988). 'Combining Qualitative and Quantitative Methods inInformation Systems Research: A Case Study', *MIS Quarterly*, **12**(4), pp. 570-587.

Kardell, R. L. (2007). 'Three Steps to Fraud Prevention in the Workplace'. ACFE Report to the Nation of Occupational Fraud and Abuse, pp. 16-19.

Karn, J. (2013). 'Policing and Crime Reduction: The evidence and its implications for practice', Police Effectiveness in a Changing World Project, pp.1-36. Available online at http://www.police-foundation.org.uk/uploads/catalogerfiles/policing-and-crime-reduction/police-foundation-police-effectiveness-report.pdf, accessed 24/06/2014.

Katz, D. and Kahn, R.L. (1966). (edn). *The social psychology of organizations*. New York: Wiley.

Kee, C, K. (2001). 'Security Policy Roadmap - Process for Creating Security Policies'. SANS Institute InfoSec Reading Room, Version 1, pp. 1-10.

Keeney, M. M. et al. (2005). 'Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors'. Joint SEI and U.S. Secret Service Report, Pittsburgh, PA, p. 1-45.

Keirns, N., Strayer, E., Griffiths, H., Cody-Rydzewski, S., Scaramuzzo, G., Saddler, T. and Vyain, S. (2013). (edition). Sociological Research, In: Introduction to Sociology, pp.31-49.

Kelle, U. (2001). 'Sociological Explanations between Micro and Macro and the Integration of Qualitative and Quantitative Methods. Forum: Qualitative Social Research'. Retrieved Available at http://www.qualitative-research.net/fqs-texte/1-01/1-01kelle-e.htm; Accessed on 12 March 2012.

Kemmis, S, and McTaggart, R. (2000). *Participatory Action Research*. In: N. K. Denzin, and Lincoln, Y. S. (Eds.), *Handbook of Qualitative Research*, 2nd ed. Thousand Oaks: Sage.

Kim, C., Newberger, B. and Shack, B. (2012). 'Computer Crimes', *American Criminal Law Review*, **49**(2), pp. 1-142.

Kimble, C. and Hildreth, P. (2004). *Knowledge Networks: Innovation through Communities of Practice*. US: Idea Group Inc.

King, M. (2006). *What's the Use of Luhmann's Theory?* In M. King and C. Thornhill (eds), *Luhmann On Law and Politics*, pp. 46-47. UK, Oxford: Hart.

Klein, H., and Hirschheim, R. (1989). 'Legitimation in information systems development: a social change perspective'. *Office: Technology and People*, **5**(1), pp. 29–46.

Kluckhohn, F, R. (1940). 'The Participant-Observer Technique in Small Communities', *American Journal of Sociology*, **46**(3), pp. 331-343.

Koh, Ruighaver, A. B., Maynard, S. B. and Ahmad, A. (2005). 'Security Governance: Its Impact on Security Culture'. *Proceedings of 3rd Australian Information Security Management Conference*, pp. 47-56.

Koops, B. J, Leenes, R., Meints, M., van der Meulen, N., and Jaquet-Chifelle, D. (2009). 'A typology of identity-related crime: Conceptual, technical, and legal issues'. *Information, Communication and Society,* **12**(1), pp. 1-24.

Koops, B. J. and Ronald, L. (2006). 'Id theft, Id fraud and/or Id-related crime: definitions matter'. Datenschutz und Datensicherheit.

KPMG. (1997). 'Business Organisations' Fraud Survey'. KPMG Report, Sydney: Australia.

Kramer, F. D., (2009). 'Policy Recommendations for a Strategic Framework'. In: Cyberpower and National Security, ed. Franklin D. Kramer *et al*., Dulles: National Defence University Press and Potomac Books, Inc., 15.

Krippendorff, K. (1980). *Content Analysis: an introduction to its methodology*. Newbury Park and London: Sage.

Kroll Global Fraud Report (2010), Available at: http://ethicsline.com/pdf/kroll-global-fraudreport-english-us-apr10.pdf, Accessed 23 September 2011.

Kroll Global Fraud Report. (2013). http://fraud.kroll.com/wp-content/uploads/2013/10/ FraudReport_2011-2012.pdf; Accessed 08 February 2013.

Kuhn, T. (1970). . (2nd edn). *The structure of scientific revolutions*. Chicago, IL: University of Chicago Press.

Lacey, D. and Cuganesan, S. (2005). 'The Role of Organisations in Identity Theft Response: The Organization–Individual Victim Dynamic'. *Journal of Consumer Affairs.* **38**(2).

Lacoste, J., and P. Tremblay. (2003). 'Crime Innovation: A Script Analysis of Patterns in Check Forgery'. *Crime Prevention Studies*, 16, p.171–198.

Ladson-Billings, G. (2003). *Radicalised discourses and ethnic epistemologies*. In N. K. Denzin and Y. S. Lincoln (Eds.), *The landscape of qualitative research: Theories and issues,* pp. 398-432. Thousand Oaks, CA: Sage.

Lanier, C. D. and Saini, A. (2008). 'Understanding Consumer Privacy: A Review and Future Directions'. Available at: http://www.amsreview.org/articles/lanier02-2008.pdf. Accessed 13 February 2012.

Lather, P. (1992). 'Critical frames in educational research: Feminist and post-structural perspectives'. *Theory into Practice,* **31**(2), pp. 87-99.

Lather, P. (2004). *Research as praxis*. In R. A. Caztambide-Fernandez, H. A. Harding, and T. Sorde-Marti (Eds.), *Cultural studies and education: Perspectives on theory, methodology, and practice,* 38, pp. 41-60). Cambridge, MA: Harvard Educational Review.

Laudise, T. M. (2008). 'Ten practical things to know about 'sensitive' data collection and protection'. *The Computer and Internet Lawyer*, **25** (7), pp. 26-33.

Lawrence, T. and Suddaby, R. and Leca, B. (2009). 'Institutional Work: Refocusing Institutional Studies of Organisation'. *Journal of Management Inquiry*, **20**(1), pp. 52-58.

Layder, D. (1993). *New Strategies in Social Research,* Polity Press: Cambridge.

Le Lievre, E., and Jamieson, R. (2005). 'An Investigation of Identity Fraud in Australian Organisations'. Collaborative Electronic Commerce Technology and Research (CollECTeR), pp. 1-10.

Lee, D. and Newby, H. (1989). *The problem of sociology. An introduction to the discipline.* London: Unwin Hyman.

Leidner, D. E. and Schultze, U. (2002). 'Information Systems Research and Knowledge Management: Theoretical Assumptions'. *MIS Quarterly*, **26** (3), pp. 213-240.

Leon, J. F. (2008). 'Top Ten Tips to combat Cybercrime'. *The CPA Journal.* **78**(5), pp. 6-19.

Leslie, C., Hood, A., (2009). *Circling the Loan Sharks: Predatory Lending in the Recession and the Emerging Role for Local Government*. London: New Local Government Network.

Levin, M. A., (1971). 'Policy Evaluation and Recidivism', *Law and Society Review*, **6**(1), pp. 17-46.

Lewins, A. and Silver, C. (2007). *Using Software in Qualitative Research*, London: SAGE Publications.

Lewis, E.R and T.T. Sullivan (1979). 'Combating Crime and Citizen Attitudes: A Study of the Corresponding Reality'. *Journal of Criminal Justice*, 7, pp. 71-79.

Li, J. (2007). 'Women's ways of gambling and gender-specific research'. *Sociological Inquiry, 77*, pp. 626-636.

Li, J. (2008). 'Ethical Challenges in Participant Observation: A Reflection on Ethnographic Fieldwork'. *The Qualitative Report, **13***(1), pp. 100-115.

Listerman, R. A., and Romesberg, J. (2009). 'Creating a culture of security is key to stopping a data breach. Are we safe yet?' *Strategic Finance*, pp. 27-33.

Lockheed and Hutchin. (2010). Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Available at http://www.ciosummits.com/LM-White-Paper-Intel-Driven-Defense.pdf, Accessed on 29 July 2013.

London, M. (1999). 'Principled leadership and business diplomacy: a practical, values-based direction for management development', *The Journal of Management Development*, 18(2), pp. 170-89.

Lu. Y and Ramamurthy. K. (2011). 'Understanding the Link between Information Technology Capability and Organizational Agility: An Empirical Examination'. *Management Information System Quarterly*, **35** (4), pp. 931-954.

Luhmann N. (2004). *Law as a Social System*. pp. 64-66. Oxford: Blackwell, UK.

Lupu, E. C. and Sloman, M. (1997). 'Towards a Role Based Framework for a Distributed Systems Management', *Journal of Network and Systems Management*, **5**(1), pp.1-17.

Lyytinen, K. (1987b). *A taxonomic perspective of information systems development: Theoretical constructs and recommendations*. In: Boland, R. and Hirschheim (Eds), *Critical issues in Information Systems Research*, pp. 3-41. Chichester: Wiley.

MacInnes, I., Musgrave, D., and Laska, J. (2005). 'Electronic Commerce Frauds: Towards: An Understanding of the Phenomenon'. In Proceedings of the 38th Annual Hawaii International Conference.

Madan, P. and Starkey, K. (2001). 'Bridging the Relevance Gap: Aligning Stakeholders in the Future of Management Research'. *British Journal of Management*, **12**(1).

Madsen, M.T. (2002) 'Managerial roles in a dynamic world', Proceedings of the 12th Nordic Conference on Small Business Research, Finland.

Manning, P.K. (1989). *Occupational Culture*. In Bayley, W.G, (ed.) The Encyclopaedia of Police Science. New York: Garfield. Manning, P.K. (1995). 'The Study of Policing', *Policing and Society*, **8**(1), pp. 23-43.

Mars, G. (1974). '*Dock pilferage: A Case Study in Occupational Theft*.' In: P. Rock and M. McIntosh (eds), *Deviance and Social Control*, pp. 209–28. London: Tavistock

Mars, G. (1982). *Cheats at Work: Anthropology of Workplace Crime*, London: Allen and Unwin.

Mars, G. (2006). 'Changes in Occupational Deviance: Scams, Fiddles and Sabotage in the Twenty-First Century'. *Crime, Law and Social Change*, **2006**(45), pp.285-296.

Mars, G. (Ed.) (2001a). *Sabotage.* Aldershot: Ashgate.

Mars, G. (Ed.) (2001b). *Occupational crime*. Aldershot: Ashgate.

Marshall, C. and Rossman, G. (3rd edn.). (1999). *Designing Qualitative Research*, Thousand Oaks: Sage.

Mathiassen, L. Munk-Madsen, M. Nielsen, P. A. Stage, J. (1991). *Soft systems in software design,* In: Jackson, M, et al. Systems thinking in Europe, pp. 311–318. New York: Plenum.

Maynard, S. B., and Ruighaver, A. B. (2006). 'What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality'. *In Proceedings of the fifth annual security conference,* Las Vegas, Nevada USA.

Mayne, J. and J. Hudson (1992). *Programme Evaluation: An Overview*, In: J. Hudson, J. Mayne and R. Thomlison (eds.), *Action-oriented Evaluation in Organisations: Canadian Practices.* Toronto, CAN: Wall and Emerson.

McConville, M. and Shepherd, D. (1992). *Watching Police, Watching Communities*, London: Routledge.

McCormick, M. (2008). 'Data Theft: A Prototypical Insider Threat'. *Advances in Information Security,* **39**(2008), pp.53-68.

McCrossan, L. (1991). *A Handbook for Interviewers*. London: Sage.

McDonald, G. and Nijhof, A. (1999). 'Beyond Codes of Ethics: An Integrated Framework for Stimulating Morally Responsible Behaviour in Organisations', *Leadership and Organization Development Journal*, **20**(3), pp. 133–146.

McDonald, P. P., Peed, C. R., Frazier, T. and Hurtt, H. (2006). 'National Strategy to Combat Identity Theft'. A Final Technical Report.

McLaren, T. S., Head, M. M., Yuan. Y., and Chan, Y. E. (2011). 'A Multilevel Model for Measuring Fit between a Firm's Competitive Strategies and Information Systems Capabilities'. *Management Information System Quarterly*, **35** (4), p. 909-929.

Mercuri, R. T. (2005). 'Challenges in Forensic computing'. *Communication of ACM*, **48**(12), pp. 17-21.

Merriam, S. B. (1988). *Case Study Research in Education: A Qualitative Approach*. San Francisco: Jossey-Bass.

Meulen, N. (2006). 'The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European Union International'. Victimology Institute Tilburg (INTERVICT), Report Commissioned by the National Infrastructure Cyber Crime program (NICC).

Meulen, N. (2011). 'Financial Identity Theft: Context, Challenges and Countermeasure'. *Information Technology and Law Series*, pp. 25-36

Meyers, M. and Rogers, M. (2004). 'Computer Forensics: The Need for Standardisation and Certification'. *International Journal of Digital Evidence,* **3**(2), p. 1-11.

Miles, M. and Huberman, A. (1985). *Assessing local causality in qualitative research. Exploring Clinical Methods for Social Research*. Beverly Hills: Sage.

Mills, G. (2007). *Identity Theft: Everything you need to know to protect yourself*. Sussex, UK: Summersdale Publishers.

Mitnick, K. D., and Simon W. L. (2006). *The Art of the Intrusion: Real stories behind the exploits of hackers, intruders and deceivers.* U.S: Wiley Publishing Inc.

Mitroff, I. and Mason, R. (1973). 'A programme for research on management information systems'. *Journal of Management Science*, 19, pp. 475-487.

Mitzberg, H. (edn). (1997). *The Nature of Managerial Work*. Prentice Hall, pp. 76-102.

Moore, A. P. et al. (2008). 'Combating the Insider Cyber Threat'. *IEEE Security and Privacy,* **6**(1), pp. 61-64.

Moore, A. P. et al. (2008). 'The Big Picture of Insider IT Sabotage across U.S. Critical Infrastructures'. Tech Rep CMU/SEI-2008-TR-009.

Moore, R. (2005). *Cybercrime: Investigating High-Technology Computer Crime,* Cleveland, Mississippi: Anderson Publishing.

Moorthy, M. K., Seetharaman, A., Zulkifflee, M., Meyyappan, G., and Lee, H. S. (2011). 'The impact of information technology on internal auditing'. *African Journal of Business Management,* **5**(9), pp. 3523-3539.

Morgan, P, M., (2010). 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', Paper presented at a workshop on deterring cyber-attacks, Washington, DC, 57.

Morris II, R. G. (2004). 'The Development of an Identity Theft Offender Typology: A Theoretical Approach'. Available at: http://www.shsu.edu/~edu_elc/ journal/ research% 20online/re2004/Robert.pdf, Accessed on 23 August 2011.

Morse, J. (1991). 'Approaches to Qualitative-Quantitative Methodological Triangulation'. *Nursing Research*, **40**(1), pp. 120-123.

Moyer, I. L. (2001). *Criminological theory: Traditional and non-traditional voices and themes*. Thousand Oaks, CA:Sage.

MPS Operation Sterling (2009). 'Fraud Prevention Advice', Available at: http://content.met.police.uk/cs/Satellite?blobcol=urldata&blobheadername1=Content-Type&blobheadername2=Content_Disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22429%2F88%2Foperation_sterling_fraud_prevention_advice%2C0.pdf%22&blobkey=id&blobtable=MungoBlobs&blobwhere=1283598280241&ssbinary=true, Accessed on 23 June 2013.

Murphy, E. and Dingwall, R. (2002). The ethics of ethnography. In P. Atkinson, A. Coffey, S. Delamont, J. Lofland, & L. Lofland (Eds.), *Handbook of ethnography*, pp. 339-351, London: Sage.

Myers, M. D. (1997). 'Qualitative Research in Information System'. *Association for Information Research.* Available at: http://www.qual.auckland.ac.nz/. Accessed 7 December 2012.

Nair, G. S. and Riege, A. M. (1996). 'Criteria for judging the quality of case study research'. Working Paper, University of Technology, Brisbane.

National Audit Office Report. (2013). 'The UK Cyber Security Strategy: Landscape Review's Key Facts', Report by the Comptroller General, HC 890, Session 2012-2013, pp. 1-9.

National Fraud Authority Report (2013). *Annual Fraud Indicator*. London: NFA, pp. 7-32.

Nellikar, S. (2010). 'Insider Threat Simulation And Performance Analysis Of Insider Detection Algorithms With Role Based Model'. Electronic Master of Science Thesis, Electrical and Computer Engineering, Graduate College of the University of Illinois at Urbana-Champaign. USA. pp. 1-6. Available at: https://www.ideals.illinois.edu/bitstream/handle/2142/16177/Nellikar_Suraj.pdf?sequence=2. Accessed on 23 May, 2011.

Neuman, W. L. (1994). *Social Research Methods*. Needham Heights: Allyn and Bacon.

Newburn T. and Webb, B. (1999). 'Understanding and preventing police corruption: Lessons from the literature', *Home Office Policing and Reducing Crime Unit Research* and Reducing Crime Unit: Police Research Series, pp. 1-45.

Newman, G. R. (2004). 'Identity Theft, Problem-Oriented Guides for Police, Problem-Specific Guides Series. U.S. Department of Justice, 25.

Newman, G. R., and McNally, M. M., (2005). 'Identity Theft Literature Review'. U. S Department of Justice, Washington, D.C.

Newman, G., and Clarke, R. (2003). *Superhighway Robbery: Preventing E-Commerce Crime.* London: Willan.

Newman, K. (1984). *Report for the Commissioner of the Metropolis 1983*. London, UK: Her Majesty's Stationery Office.

Nicklin, T., Meyer, K., Hardy, R. and Wilkins, N. (2013). *Cambridge Marketing Handbook: Digital - Cambridge Marketing Handbooks)*. Kogan Page Publishers: London. pp. 12-15.

Niekerk, R. and Solms, R. V. (2010). 'Information security culture: A management perspective'. *Computers and Security*, **29**(4), pp. 476-486.

Nieminski, J. (2008). 'Access and security internal control review'. Internal control review report, 08-3. Audit of HTE and Lenel system access and security, Gresham city.

O'Neill, O. (2002) *A question of trust.* Cambridge: CUP.

Obergfell-Fuchs, J. and Kury, H. (edn). (2003). *Crime Prevention: New Approaches*. Mainz, De. Weisse Ring Verlag-GmbH.

Office for National Statistics (ONS), (2014). Report for Crime in England and Wales. Available at: http://www.ons.gov.uk/ons/rel/crime-stats/crime- statistics/period-ending-march-2014/index.html, Accessed on 22 August 2014.

Oltsik, J. (2012). 'Enterprise Information Security in Transition: An Opportunity for IBM, Enterprise Strategy Group'. Available at: http://www.esg-global.com/briefs/enterprise informationsecurity-in- transition-an-opportunity-for-ibm, Accessed on: 27 October 2011.

Onwuegbuzie, A,J. Dickinson, W,B. Leech, N,L. Zoran, A,J.(2009). "A Qualitative Framework for Collecting and Analyzing Data in Focus Group Research". *International Journal of Qualitative Methods*, **8**(3), pp.1-15.

Organisation for Economic Cooperation and Development (OECD), (2013). 'OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data'. Available at: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf, Accessed 30 November 2013.

Organisation for Economic Cooperation and Development (OECD), (2008). 'Policy Guidance on Online Identity Theft'. OECD Ministerial Meeting on the future of the Internet Economy Seoul.

Organised Crime Strategy Report. (2005-2009). Available at www.police.vic.gov.au/retrievemedia.asp?Media_ID=2544, Accessed 04 June 2012.

Orlikowski, W., and Baroudi, J. (1991). 'Studying information technology in organisations: research approaches and assumptions'. *Information Systems Research*, **2**(1), pp. 1–28.

Orsagh, T. and Chen, J, R. (1988). 'The Effect of Time Served on Recidivism: An Interdisciplinary Theory', *Journal of Quantitative Criminology,* **4**(2), pp. 155-171.

Outhwaite, W. (1983). *Toward a realist perspective*. In: G. Morgan (edn.) *Beyond Method: Strategies for Social Research*, pp. 321-330. Beverly Hills: Sage.

Owen, J.M. and P.J. Rogers. (2nd edn.). (1999). *Programme Evaluation: Forms and Approaches.* St Leonards, New South Wales, AUS: Allen and Unwin.

Paoline, E. A. (2003). 'Taking stock: Toward a richer understanding of police culture', *Journal of Criminal Justice*, **31** (2003), pp. 199-214.

Park, J. S. and Giordano. J. (2006). 'Role-Based Profile Analysis for Scalable and Accurate Insider-Anomaly Detection'. Proceedings of the 25th IEEE International Performance Computing and Communications Conference, Workshop on Information Assurance, Phoenix, AZ, pp. 463-469.

Parker, D. (1998). *Fighting Computer Crime: A New Framework for Protecting Information.* Wiley Computer Publishing, NY.

Passmore, D. (2009). 'Sunshine State is hacker's paradise'. The Sunday Mail, Brisbane Queensland. Available at: http://www.news.com.au/news/sunshine-state-is-a-hackers-paradise/story-fna7dq6e-1225745965102, Accessed on 17 October 2011.

Patton, M. Q. (2nd edn.) (1990). *Qualitative Evaluation and Research Methods*, Newbury Park, CA: Sage.

Paul, J. (2004). *Introduction to the Philosophies of Research and Criticism in Education and the Social Sciences.* London: Prentice Hall.

Pawson R. and Tilley N. (1997). *Realistic Evaluation*, Sage Publications Ltd

Pawson, R. and N. Tilley (1995). 'Realistic Evaluation. London', UK: Sage; In Pawson and N. Tilley (1994). 'What Works in Evaluation Research'. *British Journal of Criminology*, 34, pp. 291-306.

Pease, K. (1985). 'Crime Prevention within the Probation Service'. *Probation Journal*, 32, pp. 43-47.

Pelletier, K. L. and Bligh, M. C. (2006). 'Rebounding from Corruption: Perceptions of Ethics Programme Effectiveness in a Public Sector Organization', *Journal of Business Ethics*.

Peretti, K. K. (2009). 'Data breaches: What the underground work of 'carding' reveals'. *Sanat Clara Computer and High-Technology Law Journal*. **25**(2), pp. 375-413.

Perl, M. W. (2003). 'It's not always about the money: Why the state identity theft laws fail to Adequately address criminal record identity theft'. *Journal of Criminal Law and Criminology*, **94**(1), pp. 169-208.

Perry, C. and Rao, S. (2003). 'Convergent interviewing to build a theory in under-researched areas: principles and an example investigation of Internet usage in inter-firm relationships'. *Qualitative Market Research: An International Journal*, **6**(4), pp. 236-247.

Pettigrew, A. M. (1990). 'Longitudinal field research on change: Theory and practice'. *Journal of Organisational Science.* **1**(3), pp. 267–292.

Popa, M. and Doinea, M. (2007). 'Audit Characteristics for Information Systems'. Revista *Informatica Economică,* **4**(44), pp. 103-106.

Potter, C. and Waterfall, G. (2012). 'PriceWaterCooper's Information security breaches survey: Technical Report', Available at www.infosec.co.uk, Accessed on 15 October 2012.

Prenzler, T. (2nd edn). (2009). *Police Corruption: Preventing Misconduct and Maintaining Integrity: Advance in Police Theory and Practice Series*, CRC Press: Taylor and Francis, pp. 15-25.

PriceWaterCoopers' (PWC) (2014) Information Security Breach Survey (ISBS) Technical Report, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307296/bis-14-767-information-security-breaches-survey-2014-technical-report-revision1.pdf, Accessed on 02 April 2014.

Prosch, M. (2009). 'Preventing Identity Theft throughout the Data Life Cycle'. *Journal of Accountancy,* **207**(1), pp. 58-62.

Puhakainen, P. and Siponen, M. (2010). 'Improving Employees' Compliance through Information Systems Security Training: An Action Research Study'. *Management Information Systems Quarterly,* **34**(4), pp. 757-778.

Punch, M. (1983) 'Officers and men: occupational culture, inter-rank antagonism and the investigation of corruption' in M. Punch (ed). *Control in the Police Organisation,* Cambridge, Mass: MIT Press.

Punch, M. (1996). *Dirty Business: Exploring Corporate Misconduct.* London: Sage.

Punch, M. (2000). Politics and ethics in qualitative research. In N. K. Denzin and Y. S. Lincoln (Eds.), *Handbook of Qualitative research,* pp. 83-97. Thousand Oaks, CA: Sage.

Queensland Police Service Police (QPS) Major Fraud Investigative Group. (2009). 'Theft by Fraud. Queensland Police Service'. *Police Bulletin*, pp. 27-30.

Quinney, R. (1970). *The Social Reality of Crime*. Boston: Little, Brown.

Raab, C. D. (2008). *Social and political dimensions of identity*. In: S. Fischer-Hübner, P. Duquenoy, A. Z., and Martucci, L. (edn.). *The future of identity in the information society,* pp.3-19. New York, NY: Springer.

Ramiller, N. and Swanson, E. B. (1993). 'Information systems research thematic'. *Information Systems Research*, 4, pp. 299-330.

Ransbotham, S., Mitra, S., and Ramsey, J. (2012). 'Are Markets for Vulnerabilities Effective?' *Management Information Systems Quarterly*, **36** (1), pp. 43 – 64.

Redo, S. (2002). 'Six United Nations guiding principle to make crime prevention work'. In: Coester, M. and Marks, E. (2008). International Perspective of Crime Prevention. Forum Verlag Godesburg.

Reiner, R. (1992). *The Politics of the Police*. Hemel Hempstead: Harvester Wheatsheaf.

Reith, C. (1956*). A New Study of Police History. Edinburgh*, UK. In: Remenyi W. et al. (1998). *Doing Research in Business and Management: An Introduction to Process and Method,* London: Sage.

Remenyi, D and Williams, B, (1995). 'Some aspects of methodology for research in Information Systems', *Journal of Information Technology*, pp. 191-201.

Richards, L. (2nd Edn). (2010). *Handling Qualitative Data: a practical guide,* London: Sage.

Rix, A., Joshua, F. and Maguire, M. (2009). *Improving public confidence in the police: a review of the evidence* , 2nd ed . Home Office Research Report 28 . London : Home Office, pp. 1-4.

Rock, P. (1979). *The making of symbolic interactionism.* London: The MacMillan Press Ltd.

Romanosky, S., Telang, R. and Acquisti, A. (2008). 'Do Data Breach Disclosure Laws Reduce Identity Theft?' *Journal of Policy Analysis and Management*, **30**(2), pp. 256-286.

Rosenberg, B. (2010). 'Defence Advanced Research Projects Agency (DARPA) build Cyber Range to test security measures'. GCN: Technology, Tools and Tactics for Public Sector IT Special Report, Available at: http://gcn.com/articles/2010/06/07/ defense-it-1-cyber-range.aspx]; Accessed on 31 January 2013.

Roukis, G.S. (2006). 'Globalisation, organizational opaqueness, and conspiracy', *Journal of Management Development*, 25(10), pp. 97-980.

Rousseau, D. M., Sitkin, S. B., Burt. R. S. and Camerer, C. (1998). "Not so different after all: A cross-discipline view of trust". *Academy of Management Review*, *23*, pp. 393–404, In: Twyman, M., Harvey, N. and Harries, C. (2008). "Trust in motives, trust in competence: Separate factors determining the effectiveness of risk communication". *Judgement and Decision Making,* **3**(1), pp. 111-120.

Rowe, E. (2010). 'Trade Secrets, Data Security and Employees', *Chicago-Kent Law Review,* **84**(3), pp. 749–756.

Rowlingson, R. (2005). 'An introduction to forensic readiness planning'. Centre for the Protection of National Infrastructure (CPNI) technical note, pp. 1-13.

Salifu A. (2008). The impact of internet crime on development. *Journal of Financial Crime,* **15** (4), pp. 432-443.

Salinger M. A., Anderson, K. B., and Durbin, E. (2008). 'Identity theft'. *Journal of Economic Perspectives,* **22**(2), pp. 171-192.

Sanders, A and Young, R. (2003). *Police Powers*. In Newburn, T (ed) *Handbook of Policing*. Cullompton: Willan.

Sanders, A. and Young, R. (2002). 'From suspect to trial', In: Maguire, M., Morgan, R. and Reiner, R. (Eds), The Oxford Handbook of Criminology, Oxford University Press, Oxford.

SANS Critical Security Controls. (2008). 'Critical Security Controls for Effective Cyber Defence', Available at: http://www.sans.org/critical-security-controls/, Accessed on 20 April 2013

Sarnecki, J. (2005). 'Knowledge-Based Crime Prevention, Theoretical Points of Departure for Practical Crime Prevention'. Paper presented at the Eleventh United Nations Congress on CrimePrevention and Criminal Justice, 18 – 25 April 2005, Bangkok, Thailand, pp.1-11.

Saunders, M. N., Saunders, M., Lewis, P., and Thornhill, A. (2007). *Research Methods for Business Students,* Fourth Harlow, England: FT Prentice Hall, Pearson Education.

Savage, M. (2003). 'Former hacker Mitnick details the threat of social engineering', p. 58

Savirimuthu A. and Savirimuthu J. (2007). 'Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective'. Unscripted, UK.

Scerra, N. (2011). 'Impact of police cultural knowledge on violent serial crime investigation' *Policing: An International Journal of Police Strategies and Management*, **34**(1), pp. 83 – 96.

Scerra, N. 2011. 'Impact of police cultural knowledge on violent serial crime investigation, Policing'. *An International Journal of Police Strategies and Management*, 34, pp. 83–96.

Scherdin, M.J. (1986). 'The Halo Effect: Psychological Deterrence of Electronic Security Systems'. *Information Technology and Libraries*, pp. 232-235.

Schneier, B. (2004). *Secrets and Lies: Digital Security in a Networked*, pp. 432. John Wiley and Sons.

Schreft, S. L., (2007). 'Risks of Identity Theft: Can the market protect the payment system?' *Economic Review – Federal Reserve Bank of Kansas City*, **92** (4), pp.5-40.

Schultz, E. E. (2002). 'A framework for understanding and predicting insider attacks', *Computers and Security*, 21, pp. 526–531.

Schulze, M. and Shah, M. H. (2009). 'The step method battling identity theft using e-retailers' website'. Paper accepted at 9th IFIP Conference on e-Business, e-Services, and e-Society, I 3 E, Nancy, France.

Searle, J. R. (1979). *Expression and meaning.* Cambridge: Cambridge University Press. In: Sermon, P. A. *et al.* (2012). 'Deterring gun crime materially using forensic coatings'. *Forensic Science International*, (2012), pp. 1-6.

Sekerka, L.E. and Bagozzi, R.P. (2007), 'Moral courage in the workplace: moving to and from the desire and decision to act', *Business Ethics: A European Review*, **16** (2), pp. 132-49.

Seneviratne, M. 2004). Policing the Police in the United Kingdom, Policing & Society, 14(4), pp. 329–347.

Shah, H. M. and Okeke, R. I. (2011). 'A framework for internal identity theft prevention in retail industry'. Intelligence and Security Informatics Conference (EISIC), European, Athens, Greece.

Shah, M. and Clarke, S. (Edn). (2009). *E-banking Management: Issues, Solutions and Strategies.* IGI Global, London, UK.

Shah, M. H. and Okeke, R. I. (2012). 'Role-Based Framework as a Model for Analysing Prevention of Internal Identity Theft Related Crimes', *Submitted to Information and Management for review.*

Shah, M. H. and Okeke, R. I. and Ahmed, R. (2013). 'Issues of Privacy and Trust in E-Commerce: Exploring Customers' Perspectives', *Journal of Basic and Applied Scientific Research*, **3**(3), pp. 571-577.

Sharariri, J. A. and Lababidi, M. H. (2011). 'Factors affecting the role of internal auditor in the protection of computerised accounting Information Systems from electronic penetration (A Field Study on Banks Operating in Jordan)'. *International Research Journal of Finance and Economics,* 68, pp. 140-160.

Shearman, C. and Burrell, G. (1988). 'New Technology base firms and the emergence of new industries: some employment implications'. *New Technology, Work and Employment,* **3**(2), pp.87-99.

Sherman, L.W. (1997). 'Thinking about Crime Prevention' In: L.W. Sherman, D. Gottfredson, D. MacKenzie, J. Eck, P. Reuter and S. Bushway, 'Preventing Crime: What Works, What Doesn't, What's Promising'. Washington, DC: Office of Justice Programs, National Institute of Justice, United States Department of Justice.

Skolnick, J. (1966). *Justice without Trial: Law Enforcement in Democratic Society*. New York: Macmillan College Division.

Slapper, G. and Tombs, S. (1999). *Corporate Crime*. Longman Criminology Series, Pearson Education Ltd, Harlow.

Slosarik, K. (2002). 'Identity theft: An overview of the problem'. *The Justice Professional*, **15**(4), pp. 329-343.

Smircich, L. and Morgan, G. (1980). The Case for Qualitative Research. *Academy of Management Review*, **5**(4), pp. 491-500.

Smith A. E and Humphreys, M. S (2006). 'Evaluation of Unsupervised Semantic Mapping of Natural Language with Leximancer Concept Mapping'. *Behaviour Research Methods, Instruments and Computers,* **38** (2), pp. 262-279.

Smith, L. and Laycock. G. (1985). 'Reducing Crime: Developing the Role of CrimePrevention Panels. London. UK: Home Office Crime Prevention Unit'. In: K.Pease. (1985). 'Crime prevention within the probation service'. *Probation Journal,* 32, pp. 43-47.

Smith, M. J. (1998). *Social science in question*. London: Sage Publications Ltd.

Smith, P.K. (2000). *Philosophy of Science and its relevance for the Social Sciences*; In: Burton D. (Ed.), *Research Training for Social Scientists*. Thousand Oaks, Sage.

Smith, R.E. (1988). 'The logic and design of case study research'. *The Sport Psychologist,* 2, pp. 1-12.

Sokolov, A. P. (2005). *Identity Theft on the Rise.* US: Nova Science Publishers Inc.

Sommer, P. (3rd edn.). (2012). 'Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers'. Information AssuranceAdvisory Council, UK.

Sonnenwald. D.H. Managing cognitive and affective trust in the conceptual R&D organization. In. M. Livonen and M. Huotari. (Eds.). *Trust in knowledge management and systems in organizations.* pp.82-106. Hershey, PA: Idea Publishing.

Spradley, J, P. (1980). Participant Observation. Orlando, Florida: Harcourt College Publishers, pp. 58–62.

Spradley, J. P. (1980). Participant observation. New York, NY: Holt, Rinehart & Winston.

Stake, R. E. (2000). *Case Studies.* In: Denzin, N. K. and Lincoln, Y. S. (Edn). *Handbook of Qualitative Research*, (2nd edn.). Thousand Oaks: Sage.

Stake, R.E. (1967). 'The Countenance of Educational Evaluation'. *Teachers College Record,* 68, pp. 523-540.

Stake, R.E. (1994). *Case Studies: Handbook of Qualitative Research*, Sage: Thousand Oaks.

Stake, R.E. (1995). *The Art of Case Study Research,* Sage; Thousand Oaks.

Steinbart, P. J, Raschke, R, L. Gal, G. and Dilla, W. N. (2011). 'The Relationship between Internal Audit and Information Security: An Exploratory Investigation'. University of Waterloo Centre for Information Integrity & Information Systems Assurance 7th Biennial Research Symposium, October 20-22, 2011, pp. 1-32

Steinnon, R. (2006). 'Ignoring the insider threat'. *Trade Publication: Network World.* **23**(33), p. 58.

Stickley, J. (2009). *The Truth about Identity Theft. Why be me when I can be you?* New Jersey: Pearson Education.

Straub, D. (1986). *Deterring Computer Abuse: The Effectiveness of Deterrent Countermeasures in the Computer Security Environment*. Bloomington, IN: Indiana University School of Business.

Strauss, A. and Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques,* CA: Sage Publications.

Strauss, A. and Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage.

Sutton, A. Cherney, A. and White, R. (2013). *Crime Prevention: Principles, Perspective and Practices*, Cambridge University Press, pp.1-276.

Swartz, N. (2008). 'Officials Crack Largest ID theft Ring Ever'. *Information Management Journal,* **42**(6), p. 18.

Symonenko, S., Liddy, E. D., Yilmazel, O., Zoppo, R. D. and Brown, E. (2004). 'Semantic analysis for monitoring insider threats'. IEEE International Conference on Intelligence and Security Information.

Taylor, R. B., Goldkamp, J. S., Weiland, D., Breen, C., Garcia, R. M., Presley, L. A. Wyant, B. R. (2007). 'Revise policies mandating offender DNA collection'. *Criminology and Public Policy*, **6**(4), pp. 851–862.

Taylor, S.J., and Bogdan, R. (2000). Introduction to Qualitative Research Methods. Buenos Aires: Policy Press.

TechNet Blogs. (2013). 'Introducing Enhanced Mitigation Experience Toolkit (EMET) 4.1', Available at: http://blogs.technet.com/b/srd/archive/2013/11/12/introducing-enhanced-mitigation-experience-toolkit-emet-4-1.aspx, Accessed 22 December 2013.

Thompson, P. and McHugh, D. (4 edn). (2009). *Work Organisations: A critical approach*. Chippenham and Eastbourne: Palgrave Macmillan.

Tójar, J. C. (2006). *Qualitative Research: Understanding and Doing*. Madrid: La Muralla.

Tonry, M. (2008). *Learning from the Limitations of Deterrence Research*, In: Crime and Justice: A Review of Research edited by M. Tonry. The University of Chicago Press.

Tsai, J. L. (2001). 'Cultural orientation of Hmong young adults'. *Journal of Human Behaviour and the Social Environment,* **3**(4), pp. 99-114.

Tsiakis, T. (2009). 'Contribution of corporate social responsibility to information security management'. *Information Security Technical Report*, **14**(4), pp.217 – 222.

Tucker, J. (1989). 'Employee theft as a social control'. *Journal of Deviant Behaviour,* **10**(4), pp. 319-334.

Tucker, J. (1989). 'Employee theft as social control'. *Deviant Behaviour,* 10, pp. 319-334.

Udo, G. J. (2001). 'Privacy and security concerns as major barriers for e-commerce: a survey study'. *Information Management and Computer Security*, **9**(4), pp. 165-174.

UK Crime and Disorder Act. (1998). 'Crime Prevention and Disorder, Part 1, Section 6: Formulation and Implementation of Strategies'. Available at http://www.legislation.gov.uk/ukpga/1998/37/part/I, Accessed 13 October 2011.

UK Foresight (2000). 'From a nation of shopkeepers to a world of opportunities'. Available at:http://www.bis.gov.uk/assets/foresight/docs/retail-and-consumer-services/retail revolution-dec-2000.pdf, Accessed 10 July 2011.

UK Fraud Advisory Panel. (2nd edn). (2011). 'Fraud Facts, Information for Individuals'. 1, pp.1-2.

UK Home Office Crime Prevention Unit. (1986). *Crime Prevention and the Community Programme.* London, UK. In: UK Home Office (1985) *Crime Prevention Initiatives in England and Wales*, London: UK.

UK Home Office. (2004). *Forensic Science Pathfinder Project: Evaluating Increased Forensic Activity in GMP and Lancashire.* London, UK: Author.

UK National Audit Office Report. (2013). 'Cost of Cybercrime (2013)'. https://www.gov.uk/goverment/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

Vacca, J. R. (2003). *Identity Theft*. USA: Prentice Hall PTR.

Valrie, C. and Rabih, Z. (2013). 'Stopping Tax Identity Theft: Practical Advice for CPAs and Clients: Learn Preventive Actions and Ways to Correct Problems after a Thief Has Struck'. *Journal of Accountancy*. 215(2), pp. 1-6.

Van Maanen, J. (1974). Working the Street: 'A Developmental View of Police Behaviour'. In Jacob, H (ed.). 'The Potential for Reform of Criminal Justice'. *Sage Criminal Justice System Annual Review*, 3. California: Sage.

Van Maanen, J. (1988). *Tales of the Field: On Writing Ethnography*. Chicago: University of Chicago Press

Vasiu, L. (2004). 'A Conceptual Framework of eFraud Control in an Integrated Supply Chain'. Proceedings of European Conference on Information Systems (ECIS), Paper 161.

Verizon RISK Team Survey Report. (2012). 'Data Breach Investigations Report'. Available at: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report2012_en_xg.pdf, Accessed 23 April 2013.

Verizon, (2013). 'Data Breach Investigation Report'. Available at: http://www.verizonenterprise.com/resources/reports/dbir-series-why-businesses-are-attacked_en_xg.pdf, Accessed 27 December 2013.

Verizon, (2014). 'Data Breach Investigation Report'. Available at: rp_Verizon-DBIR-2014_en_xg%20.pdf, Accessed 3 May 2014.

Vinten, G. (1994). 'Participant Observation: A model for organisation Investigation'. *Journal of Managerial Psychology*, **9**(2), pp. 30 – 38.

Waddington, P.A.J. (1999a) Policing Citizens: Authority and Rights. London: Routledge.

Walker, A., Flatley, J., Kershaw, C and Moon, D. (2008,09). Crime in England and Wales: Findings from the British Crime Survey and police recorded crime, Home Office Statistical Bulletin Volume 1, pp. 85-87.

Walker, C. (2006). Computer forensics: bringing the evidence to court. Available at :http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pd]; Accessed 24 January 2013.

Wallace, L., Lin, H., and Cefaratti, M. A. (2011). 'Information security and sarbanes-oxley compliance: an exploratory study'. *Journal of Information Systems*, **25**(1), pp. 185-211.

Walliker, A. (2006). 'Identity Theft soars and now costs $3 billion a year', Sunday Hearld-Sun. Melbourne Victoria, p. 88.

Walsham, G. (1995). 'Interpretive Case Studies in IS Research: Nature and Method'. *European Journal of Information Systems*, 4, pp. 74-81.

Wang, G., Chen, H., and Atabakhsh, H. (2004). 'Criminal Identity Deception and Deception Detection in Law Enforcement'. *Group Decision and Negotiation*, 13, pp. 111-127.

Wang, W., Yuan, Y., and Archer, N. (2006). 'A contextual Framework for Combating Identity Theft, IEEE Security and Privacy'. Published by IEEE Computer Society.

Ward, P. T., and Anand, G., and Tatikonda, M. V. (2010). 'Role of explicit and tacit knowledge in six sigma projects: An empirical examination of differential project successes. *Journal of Operations Management,* **28** (4), pp. 303-315.

Warren, P. and Streeter, M. (2005). *Cyber Alert: How the world is under attack from a new form of crime*. London: Vision.

Weick, K. (1995). *Sensemaking in Organisations*. Thousand Oaks: Sage.

Welch, T. (1997). 'Computer crime investigation and computer forensics'. *Information systems security*, **6**(2), pp. 25-56.

Wells, J. (2010). 'ACFE Report', *Journal of Accountancy*, pp. 1-82.

Wenger, E. (1998). *Communities of practice: learning, meaning, and identity*. Cambridge University Press.

Wenger, E., McDermott, R. and and Snyder, W. (2002) .*Cultivating communities of practice: a guide to managing knowledge*. Harvard Business School Press.

Westley, W. (1970). *Violence and the Police.* Cambridge, MA: The Free Press.

Widup, S. (2010). 'The Leaking Vault: Five Years of Data Breaches', *Digital Forensics Association*, pp. 1- 42.

Wilkinson, S. and Haagman, D. (2011). 'Good Practice Guide for Computer-Based Electronic Evidence'. Association of Chief Police Officer (ACPO): 7Safe Information Security, Official Release, pp. 6-72.

Williams, K. R., Gibbs, J. P., Erickson, M. L. (1980). 'Public Knowledge of Statutory Penalties: The Extent and Basis of Accurate Perception', *Pacific Sociological Review,* **23**(1).

Willison, R. (2006). 'Understanding the perpetration of employee computer crime in the organisational context'. *Information and Organisation* **16**(4). pp. 304-324.

Willison, R. and Backhouse, J. (2006). 'Opportunities for computer crime: Considering systems risk from a criminological perspective'. *European Journal of Information Systems* 15, (4), pp. 403-414.

Willson, J. Q., and Herrnstein, R. J. (1985). *Crime and human nature.* New York: Simon and Schuster.

Wilson, J. (2010). *Essentials of Business research: A Guide to doing your Research Project.* London: SAGE.

Wilson, T.D. and Streatfield, D.R. (1977). 'Information needs in local authority social services departments: an interim report on project INISS'. *Journal of Documentation,* **33**(4), pp. 277-293.

Wortley, R. (1997). *Reconsidering the Role of Opportunity in Situational Crime Prevention*, UK: Ashgate. pp. 65-81.

Wright, M. A. (1998). 'The Need for Information Security Education'. *Computer Fraud and Security*, pp.14-17.

Wright, V. (2010). 'Deterrence in Criminal Justice Evaluating Certainty vs. Severity of Punishment'. The Sentencing Project Research and Advocacy for Reform, pp.1-9.

Yang, S. and Wang, Y. (2011). System Dynamics Based Insider Threats Modelling, *International Journal of Network Security and Its Applications*, **3**(3), pp. 1-12.

Yeager, P.C., (2007). *Understanding corporate law breaking: from profit seeking to law finding.* In: Pontell, H., Geis, G. (Eds.), *International Handbook of White-Collar Crime.* Springer, New York.

Yin, R. K. (1981). 'The case study as a serious research strategy'. *Knowledge: Creation, Diffusion, Utilisation*, **3**(1), pp. 97-114.

Yin, R. K., (1984). *Case study research: Design and methods*. Sage, New York.

Yin, R. K. (1989). *Case Study Research Design and Methods*. Newbury Park: Sage.

Yin, R. K. (1993). *Applications of Case Study Research*. Newbury Park: Sage.

Yin, R. K. (2nd edn.). (1994). *Case Study Research: Design and Methods*. Thousand Oaks: Sage.

Yin, R. K. (3rd edn). (2003). *Case study research: Design and methods*. Thousand Oaks, CA: Sage.

Yuan, L. (2005). 'Companies face system attacks from inside, too'. *The Wall Street Journal Online.*

Zhang, Y. and Yin, J. (2006). 'A Role-Based Modeling for Agent Teams'. Proceedings of 2006 IEEE Workshop on Distributed Intelligent Systems - Collective Intelligence and Its Applications, Prague, Czech.

Zhu, H. (2006). 'Introduction to the Special Session on Role-Based Collaboration'. Distributed Intelligent Systems: Collective Intelligence and Its Applications, IEEE Workshop. Conference Publications, pp. 335-336.

APPENDIX

Appendix 1: Review Framework

A1: Scope of the Review

In the review of the literature, the following were explored: most cited definitions of identity theft related crimes (IIDTRC), situations that encourages employees to perpetrate IIDTRC online retail, the state of IIDTRC in UK, and other countries, the method of propagation of this crimes and their corresponding recommend countermeasures.

A2: Lines of Enquiry

What is the extent of internal identity theft related crimes (IIDTRC) in UK?
What are the methods used by employees to steal/accidental leak customers' data?
What are the methods that are being used to prevent IIDTRC in UK or elsewhere?
Who is responsible for preventing IIDTRC in online retail?
What stage has the online retail companies reached in developing its IIDTRC prevention capacity?
What IS security practices/strategies in place in terms of IIDTRC prevention framework, e.g. departmental responsibility, IT security tools, laws, monitoring systems, policies, human resources, programmes and training?
What are the major IIDTRC concerns the online retail has or wishes to tackle?
What are the main vulnerabilities at greatest risk of lapsing into IIDTRC or becoming the subject of IIDTRC victimization?
What are the main areas of concentration of IIDTRC problems?
What are the main retail business operations affected by the IIDTRC incidents?
What online management capability and capacity exist to develop and sustain strategic IIDTRC prevention?
What exists in terms of recent or current human resources, technical or procedural assistance in preventing IIDTRC?
What is the principle/rule of law in prevention of IIDTRC in online retail?
What is the nature of human-centred action/roles in preventing IIDTRC?
What is the state of collaboration among the management in preventing IIDTRC?
What is the nature of principle of strategic IIDTRC prevention accountability and sustainability?
Are there existing evidence-based practices in the online retail companies on prevention of IIDTRC?

A3: Search Strategy

Based on the general research framework and advised from my research director, most of the best sources for the review were selected and assessed, by browsing of relevant websites and through structured searching by applying online information and library services.

The most key websites included are those of UK government law enforcement agencies, in particular are those of UK Home Office, UK Cards Association, Her Majesty's Revenue and Customs, Metropolitan Police, National Fraud Authority; renowned research and consulting agencies in particular are those of Credit Industry Fraud Avoidance System, Financial Services Authority, Experian, Equifax, Kroll, CIPD, British Bankers Association, etc.; among other institutions' websites: website (http://www.identitytheft.org.uk). Other includes the Credit Industry Fraud Avoidance System (CIFAS), United Kingdom Home Office, Financial Fraud Action United Kingdom, United Kingdom Cards Association, Equifax, Experian, Royal Mail, CallCredit, Her Majesty's Revenue and Customs (HMRC), Driver and Vehicle Licensing Agency (DVLA), Identity and Passport Service (IPS), Serious Organised Crime Agency (SOCA), Metropolitan Police, City of London Police, Scottish Business Crime Centre, Financial Services Authority (FSA), British Banker's Association (BBA), British Security Industry Association (BSIA), National Fraud Authority (NFA). In the course of most searches of online resources and databases, index searching and a combination of free text were used. Best articles published between 2000 till dates are considered in most searches.

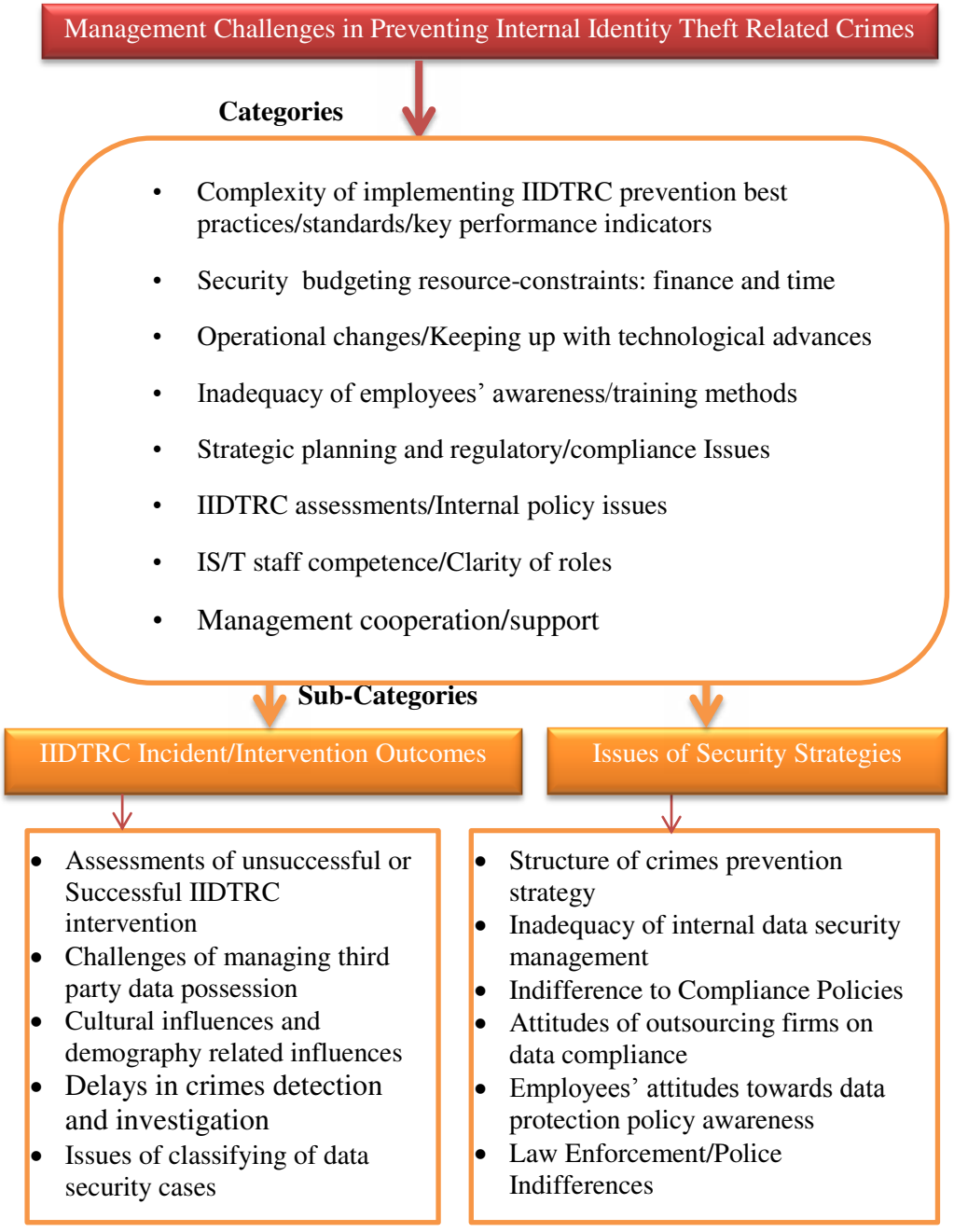
A4: Selected Cases

Some of the relevant cases of IIDTRC reported in online companies in UK are deemed imperative in this review. Studying of the cases and incidents of research problems helps to analyse that problem based on the facts. The actual and exemplary record of incidents may be helpful as the guidelines towards carrying out an intensive study of all aspects of problem selected for the research. It helps researchers and law enforcement agencies to understand the relationship of the causal factors interlinked.

The case studies narrated above are published by the CIFAS is the United Kingdom' Fraud Prevention Service CIFAS in conjunction with Charted Institute of Personal and Development.

Appendix 2: Summary of Management Challenges in Preventing IIDTRC

The diagram summarises the challenges have been the most problematic issues observed in the *RetailGroup*.



Appendix 3: Case Examples of IIDTRC Perpetrators in Banking Sector

Case #1 Personal Identity Theft Related Crimes in the Public Domain: Account Takeover/Account Withdrawal

Name	Jessica Harper
Age	50
Gender	Female
Job title	Head of Online Security/Lloyds Banking Group
Nature of fraud	Jessica Harper defrauded her Employer of almost £2.5 million in 2012. She submitted 93 false and doctored invoices to herself £2, 463, 750. She created a dummy bank account in the name of IT firm which carried out work for Lloyds.
Motivation	**Expertise**: She knew her job very well that she could create a dummy account that did not look suspicious and detectable to her employer. **Family and Social Issues:** She gave the money to her friends and her three brothers for them to buy properties. **Perception of 'Not being paid enough' at Lloyds**: Jessica denied personally benefiting from the fraud and argued that *"she deserved the money for showing "loyalty" to the firm when she could earn four times as much elsewhere",* Southwark Crown Court heard that Harper told police. She also argued that he deserved the money for working such long hours, getting up at 5.30am and getting home at around 8pm for a salary of between £60,000 and £70,000 that is not enough to carter for her family needs. **Perceived Opportunity:** She had an opportunity to be the head of online security and she perceived that she was above the law and abused her position. Detective Chief Inspector Robin Cross, from the Fraud Squad, said "*This is a serious abuse of position by a senior employee who should be protecting the bank and its customers against fraud".*
How she was caught	Jessica's fraud activities were identified and detected following an internal audit by the bank. During the investigation, it was discovered that she had previously pleaded guilty to a single charge of fraud by abuse of position and a second charge of money laundering, both between 28th December, 2007 and 21st December, 2011.

Lessons learned	i. Being head of security does necessarily exempt individual from committing fraud. ii. Past behaviour could be a good predictor of future behaviour. iii. Jessica Harper had been indicted in fraudulent act but her employer ignored the red flag and still her job. A thorough background can provide valuable information, especially when a candidate is applying for a position of trust. iv. Lack of adequate supervisory oversight and monitoring was another weakness factor. It took a "tipster's" report to identify this two-year scheme. Letting your staff know that "surprise" audits are part of your responsibilities to prevent internal fraud and embezzlement is known to be an effective strategy—that is, providing those surprise audits are regularly performed. v. Oversight: Most glaring observation was that this perpetrator had sole oversight of the company's finances, and no one ever scrutinised her management activities till her fraud was revealed. vi. Employers should apply a strict policy of internal controls, collaboration of duties and supervisory oversight irrespective of the employee position to improve company's anti-fraud programme. vii. No employee, manager or other person should have the authority to place any business project with any company, acknowledge receipt of that project and approve payment for service without employer's official authorised approval.

Case #2 Corporate Identity Theft Related Crimes in the Public Domain: Fraudulent use of company data

Name	Jérôme Kerviel
Age	33
Gender	Male
Job title	Desk trader/Banking - Société Générale

Nature of fraud	Manipulation of the share prices/hedging and price exploitation to make big profits; caused £7 billion losses in 2008 to Société Générale. Convicted for "abuse of confidence and illegal access to computers". Unauthorised and concealed trading that led to persistent unfavourable market.
Motivation	**Expertise:** Kerviel knew the timing of the nightly reconciliation process of the day's trades by Eliot (back-office trade booking system), so with his back-office credentials was able to delete and re-enter these unauthorised transactions without being noticed. He sometimes used fake counter-party information. Colleagues described him as a "computer genius" who was allegedly able to hack into the bank's computers to hide his trading, until he slipped-up. **Ambitious for promotion**: Kerviel acknowledged that he was wrong and that he has committed errors but noted that *"he was serious and efficient at work and the fact that my bosses protected me and I was promoted during my short career shows this," he says. "What's more, I never stole a single centime."* He was promoted to the bank's Delta One trading team in 2005, which specialises in the futures markets. **Avoided holidays to cover his frauds:** Kerviel took just four days of vacation in 2007; he worked around the clock of the year to prevent comprehensive audit that might uncover his fraud.
How he was caught	Kerviel's complex hidden deals were unravelled when he was trading above the bank's market value. He failed to disable the bank's automatic alert system and his irregular trading suddenly showed up and he was arrested. There should be provision for anonymous reporting across the departments. Non-segregated duties with poor internal policy and regulatory compliance and documentation.
Lessons learned	i. This fraud involves the accounting department and this confirms ACFE report cited in section 2.4.4 of literature review that over 30 per cent of the cases were committed by employee in the accounting department. ii. It is worth noting that Kerviel took just four days of vacation in 2007. It is important to require all accounting, financial and purchasing personnel to take a month off every year to avail the opportunities to audit their work activities.

Case # 3 Corporate Identity Theft in Cases in the Public Domain:

Fraudulent use of company data and unauthorised alteration to company data

Name	Kweku Adoboli
Age	32
Gender	Male
Job title	Desk trader/Banking
Nature of fraud	Manipulation of the share prices/hedging and price exploitation to make big profits. Setting up of secret bank account nickname 'umbrella' to hide losses, which exploded after his big-ever trade went sour in 2011. Caused the Swiss bank $2.3 billion loss in 2012.
Motivation	**Management Support:** Mr Adoboli line of defence was that UBS's management had encouraged him to take greater risk bring in higher profits. Mr Adoboli received only a warning for exceeding risk limits in January 2011. **Expertise:** He used his IT expertise to manipulate the system and hid the fraud trails for long time. A mechanism for verifying trades was mysteriously switched off until his fraudulent activities were exposed.
How he was caught	The bank back office discovered fake trades were booked to offset the risk created, which peaked at $12 billion in August 2011. This exposure led to his arrest in 2011.
Lessons learned	i. There was no mechanism in place that monitored Adobori's fraudulent trade exploits. There was no follow up control after warning was issued in 2011. Every business manager must ensure that appropriate internal controls, segregation of duties and supervisory oversight are in place and consistently enforced. For a single employee to have been able to prepare and issue millions of trade logs and later deposit those same fraudulent checks into his created secret personal bank account, obviously suggests that critical accounting safeguards were either not in place or seriously ignored. ii. Even if the above two steps had not been in place, had this individual's managers known what tasks to oversee and verify, and performed those tasks, this blatant crime would have been prevented or quickly detected. iii. It is also worth noting that previous financial audits also failed to identify that anything was amiss. Few managers recognise that it is common practice for an auditor's "scope of audit" not focus on detecting fraud, and this is another valid reason why management role in the fraud preventive process is so important.

Case #4 Corporate Identity Theft Related Crimes in the Public Domain: Unauthorised alteration to company's information systems

Name	John Rusnak
Age	37
Gender	Male
Job title	Desk trader/Banking – Allied Irish Banks (AIB)
Nature of fraud	Bank fraud over a trading scam that cost Allied Irish Banks (AIB) nearly $700m in trading losses. Mr Rusnak allegedly ran up the losses while trading the Japanese Yen. When the trades went against him he allegedly used fraudulent measures to cover up the losses. He also created bogus broker confirmations to validate his deals. Manipulation of the Value at Risk calculation system: Mr. Rusnak manipulated the trading software systems used by the Allfirst and AIB to monitor his trading. He did the scheme by directly manipulating the inputs into the calculation of the VaR that were used by an employee in Allfirst's risk-control group.
Motivation	**Ambition to get promoted:** Prosecutors claimed that his activities helped him to earn salary and bonuses totalling $850,000 between 1997 and 2001. **Absence of trade monitoring system in AIB:** Lack of trade monitoring system in the AIB led to the failure of the bank management to scrutinise bogus option with Asian counterparts. He took advantage of an even bigger hole in the control environment – a failure in the back-office to obtain transaction confirmations. **Negligence from management:** John Rusnak was showing a yearly profit for 5 years straight. He became untouchable in organisational politics because he appeared to be so good. The back office staff eventually gave up raising flags on his trading practices as they were continually shot down by management. With executive backing, the treasury back office could have assisted with detecting John Rusnak's fraud. **Lack of management experience on foreign exchange trading:** His supervisors were not experienced in foreign exchange trading. They did not adequately supervise his activities. A knowledgeable supervisor would have seen that the deep-in-the-money bogus options as it in Rusnak's case.

How he was caught	Rusnak frauds was revealed when AIB requested that he should release some of the capital to ease its trading balance sheet but Rusnak was not able to do that because of the heavy skew towards the forex market and that was how his whole fraudulent activities tumbled down on him and he was caught.
Lessons learned	i. The failure of the back office to attempt to confirm bogus options with Asian counter parts and obtain foreign exchange rates from an independent source. ii. There was no internal audit of treasury operations to look Rusnak's transactions to see if they had been properly confirmed. iii. In addition, AIB missed opportunities by ignoring problems ranging from problems of confirming trades and with Mr. Rusnak's personality to warnings that there was a possibility that Mr. Rusnak could be manipulating foreign exchange rates. iv. It is vital to note that AIB stock fell sharply which proved more robust than Barings that was grounded after the Nick Leeson scandal. In all this was lost to the stake holders of AIB.

Case #5 **Corporate Identity Theft Related Crimes in the Public Domain: Unauthorised alteration to company data/ modification of company payment instructions**

Name	Nicholas Leeson
Age	27
Gender	Male
Job title	Desk trader/Banking – Baring the then UK's oldest investment bank
Nature of fraud	Account fraud and forgery which involved hiding mistakes made by the 12 order fillers who worked on the trading floor. Rather, than reporting it to his bosses in London, Leeson hid the losses in a separate account known as the 'five eights' account. Mr. Leeson intentionally used the Barings' error accounts to hide the losses amounting to £827 million ($1.4 billion!) that led to 1995 collapse of Barings Bank.

Motivation	**Negligence of the supervisors:** Leeson's superior knew, or should have known what the trader was up to, having been provided with advance notice concerning his activities. Since Barings allowed him to trade and settle his trades by the end of 1994 Leeson had racked up than £200 million in losses. **No segregation of roles/power:** Leeson Case demonstrates what can happen when one individual is entrusted with too much power. There was no closer monitoring of his trading procedures: testing of positions, analysis of daily settlements and margin calls, as well as analysis of position and market concentration. **Overwhelmed by the banking business culture:** He continued to try and trade his way out of losses, behaviour he puts down to part youthful bravado and the banking culture at the time. He argued that there were some of his colleagues on the trading floor making mistakes and those mistakes very stupidly made their way back into the five eights account. Lesson said "I suppose for me as well I thought 'well it's probably not such a big deal, I got out of it once I can do it again and that was as stupid as it could possibly get". But when he to get all of the losses back - it had been as high as $20 million.
How he was caught	A routine audit by the bank as result of wiped-off of seven per cent of market because of the Kobe earthquake at the end of January 1995. Leeson said that "*the bank was running out of money or had run out of money, it was impossible to build the position anymore, markets were falling, and everything is going against me. I'm not sure if Kobe necessarily was the final nail in the coffin if you like but it certainly didn't help".*
Lessons learned	i. If there was collaboration of roles among the traders, and promotion of information sharing among trading exchanges, Leeson's fraud would have been detected earlier. ii. There was no upgraded clearing system and procedures that incorporated the real time settlement and critical risk management systems. iii. This case emphasised the need for banking companies to devise a comprehensive internal risk analysis procedures to identify high risk accounts.

Appendix 4: Publications

Portions of this thesis are published in these research papers.

Okeke, R. I and Shah, M. H. (2015), *System Security: Theft Prevention, Book to be published by July 1st, 2015, Routledge*

Shah, M. H. and Okeke, R. I. (2014). Role-Based Framework as a Model for Analysing Prevention of Internal Identity Theft Related Crimes (*submitted to Information Systems Security for review).*

Shah, M. H. and Okeke, R. I. and Ahmed, R. (2013). 'Issues of Privacy and Trust in E-Commerce: Exploring Customers' Perspectives', *Journal of Basic and Applied Scientific Research,* **3**(3), pp. 571-577.

Shah, M. H. and Okeke, R. I. (2013). Role of Digital Forensic in Identity Theft Related Crimes Investigation: The Challenges and Solutions. (*Submitted to 4th IBT International Conference).*

Shah, H. M. and Okeke, R. I. (2011). A framework for internal identity theft prevention in retail industry. In Paper presented in *Intelligence and Security Informatics Conference (EISIC).*

Appendix 5: NVivo Nodes

Internal identity theft related crimes			
Words Coded		1,049	
Created	18/05/2012 13:51	**Paragraphs Coded**	29
Modified	16/06/2012 10:19	**Coding References**	18
Sources Coded		14	
Cases Coded		14	

Identity theft			
Words Coded		189	
Created	18/05/2012 13:53	**Paragraphs Coded**	8
Modified	16/06/2012 14:20	**Coding References**	4
Sources Coded		4	
Cases Coded		4	

Causes v motives of identity theft crimes			
Words Coded		1,734	
Created	18/05/2012 13:55	**Paragraphs Coded**	47
Modified	16/06/2012 16:19	**Coding References**	23
Sources Coded		17	
Cases Coded		16	

Perpetrators of identity theft crimes			
Words Coded		1,792	
Created	18/05/2012 13:52	**Paragraphs Coded**	15
Modified	16/06/2012 10:41	**Coding**	16

References

Sources Coded 10

Cases Coded 10

carrying out identity theft crimes -Methods of

Words Coded 261

Created 08/04/2012 15:59 **Paragraphs Coded** 3

Modified 16/06/2012 14:25 **Coding References** 3

Sources Coded 3

Cases Coded 3

Internal identity theft - prevention

Words Coded 1,153

Created 18/05/2012 13:53 **Paragraphs Coded** 21

Modified 16/06/2012 14:25 **Coding References** 16

Sources Coded 12

Cases Coded 12

Security - measures - controls

Words Coded 2,026

Created 18/05/2012 13:55 **Paragraphs Coded** 44

Modified 16/06/2012 12:05 **Coding References** 30

Sources Coded 19

Cases Coded 19

different roles for different management

Words Coded 362

Created 18/05/2012 13:53 **Paragraphs Coded** 3

Modified	16/06/2012 14:20	**Coding References**	3
Sources Coded			3
Cases Coded			3

Identity theft prevention practices

Words Coded			541
Created	18/05/2012 13:54	**Paragraphs Coded**	13
Modified	16/06/2012 14:25	**Coding References**	9
Sources Coded			8
Cases Coded			8

Data security implementation processes

Words Coded			219
Created	18/05/2012 13:54	**Paragraphs Coded**	14
Modified	08/06/2012 15:15	**Coding References**	6
Sources Coded			5
Cases Coded			5

Management support in implementing data security

Words Coded			945
Created	18/05/2012 13:51	**Paragraphs Coded**	33
Modified	16/06/2012 14:25	**Coding References**	16
Sources Coded			9
Cases Coded			9

performance vs challenges – of management

		Words Coded	
18/05/2012 13:54	**Paragraphs**		

Coded			
Modified	16/06/2012 14:25	**Coding References**	30
Sources Coded		20	
Cases Coded		20	

Resources for prevention of identity theft crimes

Words Coded		109	
Created	18/05/2012 13:54	**Paragraphs**	5
Coded			
Modified	14/06/2012 14:28	**Coding References**	3
Sources Coded		2	
Cases Coded		2	

Prevention of identity theft – roles in

Words Coded		215	
Created	18/05/2012 13:54	**Paragraphs**	5
Coded			
Modified	16/06/2012 16:21	**Coding References**	5
Sources Coded		4	
Cases Coded		4	

Responsibilities of preventing crimes

Words Coded		783	
Created	20/03/2012 13:59	**Paragraphs**	3
Coded			
Modified	16/06/2012 10:19	**Coding References**	3
Sources Coded		3	
Cases Coded		3	

Management involvement – what it is

Words Coded	171

Created 18/05/2012 13:55 **Paragraphs** 3

Coded

Modified 09/05/2012 14:27 **Coding** 3

References

Sources Coded 2

Cases Coded 2

Team vs individual who is more effective

Words Coded 387

Created 18/05/2012 13:53 **Paragraphs** 8

Coded

Modified 09/05/2012 14:21 **Coding** 8

References

Sources Coded 4

Cases Coded 4

Team – performance of

Words Coded 302

Created 18/05/2012 13:53 **Paragraphs** 11

Coded

Modified 16/06/2012 16:19 **Coding** 8

References

Sources Coded 8

Cases Coded 8

Role sharing – identity prevention process

Words Coded 2,406

Created 18/05/2012 13:53 **Paragraphs** 64

Coded

Modified 16/06/2012 14:25 **Coding** 37

References

Sources Coded 19

Cases Coded 18

Management roles – clarity of

Words Coded 17

Created 18/05/2012 13:55 **Paragraphs** 1

Coded

Modified 14/06/2012 10:38 **Coding** 1

References

Sources Coded 1

Cases Coded 1

Identity theft prevention strategy

Words Coded 1,617

Created 18/05/2012 13:51 **Paragraphs** 53

Coded

Modified 10/08/2012 15:57 **Coding** 35

References

Sources Coded 22

Cases CodedV 21

Role sharing vs management interaction

Words Coded 279

Created 18/05/2012 13:53 **Paragraphs** 6

Coded

Modified 09/05/2012 11:55 **Coding** 4

References

Sources Coded 2

Cases Coded 2

Identity theft prevention policy

Words Coded 533

Created 18/05/2012 13:54 **Paragraphs** 23

Coded

Modified 16/06/2012 12:05 **Coding** 8

References

Sources Coded 6

Cases Coded 6

Management performance evaluation

Words Coded		0	
Created	28/02/2012 09:52	**Paragraphs Coded**	0
Modified	28/02/2012 09:52	**Coding References**	0
Sources Coded		0	
Cases Coded		0	

Management performance – evaluation of

Words Coded		380	
Created	18/05/2012 13:54	**Paragraphs Coded**	5
Modified	11/06/2012 17:49	**Coding References**	4
Sources Coded		3	
Cases Coded		3	

Relationships

Words Coded		3,535	
Created	08/06/2012 14:50	**Paragraphs Coded**	63
Modified	10/08/2012 15:57	**Coding References**	60
Sources Coded		18	
Cases Coded		18	

Team management challenges

Words Coded	300		
Created	18/05/2012 13:54	**Paragraphs Coded**	3
Modified	16/06/2012 14:25	**Coding References**	4
Sources Coded	3		
Cases Coded	3		

Supports

Words Coded 2,369

Created 18/05/2012 13:53 **Paragraphs** 58 **Coded**

Modified 10/08/2012 15:57 **Coding** 43 **References**

Sources Coded 20

Cases Coded 20

Management operation

Words Coded 3,148

Created 18/05/2012 13:52 **Paragraphs** 89 **Coded**

Modified 16/06/2012 16:19 **Coding** 58 **References**

Sources Coded 23

Cases Coded 22

Management-employee collaboration

Words Coded 0

Created 18/05/2012 13:50 **Paragraphs** 0 **Coded**

Modified 18/05/2012 13:50 **Coding** 0 **References**

Sources Coded 0

Cases Coded 0

Identity theft prevention practices

Words Coded 26

Created 18/05/2012 13:50 **Paragraphs** 1 **Coded**

Modified 10/06/2012 14:55 **Coding** 1 **References**

Sources Coded 1

Cases Coded 1

Collaborative management – effects of

Words Coded		220	
Created	18/05/2012 13:52	**Paragraphs Coded**	2
Modified	14/06/2012 14:28	**Coding References**	2
Sources Coded		2	
Cases Coded		2	

Roles sharing - benefits

Words Coded		385	
Created	18/05/2012 13:53	**Paragraphs Coded**	10
Modified	10/08/2012 15:57	**Coding References**	7
Sources Coded		5	
Cases Coded		5	

Management skills in organisation – effects of

Words Coded		226	
Created	18/05/2012 13:51	**Paragraphs Coded**	11
Modified	14/06/2012 11:01	**Coding References**	7
Sources Coded		6	
Cases Coded		6	

Roles sharing – process of

Words Coded		0	
Created	18/05/2012 13:54	**Paragraphs Coded**	0
Modified	18/05/2012 13:54	**Coding References**	0

Sources Coded 0

Cases Coded 0

Management roles sharing – challenges of

Words Coded 92

Created 18/05/2012 13:52 **Paragraphs** 10

Coded

Modified 14/06/2012 10:38 **Coding References** 3

Sources Coded 3

Cases Coded 3

Roles sharing vs skills

Words Coded 1,849

Created 18/05/2012 13:53 **Paragraphs** 45

Coded

Modified 10/08/2012 15:57 **Coding References** 26

Sources

Coded 21

Cases Coded 21

Data security implementation

Words Coded 483

Created 18/05/2012 13:54 **Paragraphs** 1

Coded

Modified 09/05/2012 14:21 **Coding References** 1

Sources Coded 1

Cases Coded 1

Data compliance

Words Coded 188

Created 18/05/2012 13:54 **Paragraphs** 4

Coded			
Modified	16/06/2012 10:19	**Coding References**	2
Sources Coded		1	
Cases Coded		1	

Policy enforcement

Words Coded		0	
Created	18/05/2012 13:50	**Paragraphs**	0
Coded			
Modified	18/05/2012 13:50	**Coding References**	0
Sources Coded		0	
Cases Coded		0	

Data protection policy definition

Words Coded		0	
Created	18/05/2012 13:50	**Paragraphs**	0
Coded			
Modified	18/05/2012 13:50	**Coding References**	0
Sources Coded		0	
Cases Coded		0	

clarity vs definition

Words Coded	
18/05/20 12 13:55	**Paragraphs**

Coded			
Modified	16/06/2012 14:20	**Coding References**	8
Sources Coded		8	

Cases Coded	8

Enforcement

	Words Coded		1
	36		
Created	18/05/2012 13:54	**Paragraphs Coded**	1
Modified	14/06/2012 14:28	**Coding References**	1
Sources Coded			1
Cases Coded			1

Software security

Words Coded			0
Created	18/05/2012 13:50	**Paragraphs Coded**	0
Modified	18/05/2012 13:50	**Coding References**	0
Sources Coded			0
Cases Coded			0

Software tools- integration

	Words Coded		9
	02		
Created	18/05/2012 13:53	**Paragraphs Coded**	25
Modified	16/06/2012 16:19	**Coding References**	14
	Sources Coded		
	10		
	Cases Coded		
	10		

Software security - benefits

	Words Coded		4
	06		

Created	18/05/2012 13:53	**Paragraphs Coded**	21
Modified	16/06/2012 16:19	**Coding References**	10
Sources Coded		7	
Cases Coded		7	

Software security – maintenance of

Words Coded		333	
Created	29/04/2012 10:35	**Paragraphs Coded**	8
Modified	10/08/2012 15:57	**Coding References**	8
Sources Coded		6	
Cases Coded		6	

Software security vs. management role – use of

Words Coded		1,563	
Created	18/05/2012 13:53	**Paragraphs Coded**	36
Modified	16/06/2012 14:25	**Coding References**	23
Sources Coded		16	
Cases Coded		16	

Human resources vs. software security

Words Coded		305	
Created	18/05/2012 13:53	**Paragraphs Coded**	5
Modified	16/06/2012 12:05	**Coding References**	5
Sources Coded		4	
Cases Coded		4	

Identity theft prevention reporting techniques

Created	**Words Coded** 1,029
18/05/2012 13:53	**Paragraphs Coded** 20
Modified	**Coding References** 14
14/06/2012 10:38	**Sources Coded** 8
	Cases Coded 8