Information Systems Frontiers
https://doi.org/10.1007/s10796-022-10326-w

The Application of Role-Based Framework in Preventing Internal Identity Theft Related Crimes: A Qualitative Case Study of UK Retail Companies

Romanus Izuchukwu Okeke[1] · **Max Hashem Eiza**[2]

Accepted: 12 August 2022

Abstract
This paper aims to examine the challenges of preventing internal identity theft related crimes (IIDTRC) in the UK retail sector. Using an in-depth multiple case studies of a selected number of cross-functional management teams in the UK retail companies, management roles were analysed. We used semi-structured interview as a qualitative data collection technique and used Nvivo aided thematic analysis and interpretivism underpinned by Role-Based Framework (RBF) for analysis. Our findings revealed that vagueness of roles and lack of clarity in sharing data security responsibilities are the major challenges of preventing IIDTRC in UK retail companies. We suggest an application of RBF which provides a conceptual analysis for cross-functional management team to address the challenges of preventing IIDTRC. RBF enables clarity of shared roles where both information security and crimes prevention teams work in unison is required to prevent IIDTRC to maximise internal data security. Contributions for policymakers are offered in this paper.

Keywords Internal identity theft related crimes · Data security · Role-based framework · Retail sector · Insider threat prevention · Qualitative case study

1 Introduction

The consequences of internal identity theft related crimes (IIDTRC) have become more costly as the cross-functional management of information security systems become more indispensable in the UK retail companies. The rapid growth in the use of credit and debit cards in the retail industry online and in shops leaves the consumers vulnerable to IIDTRC. These crimes pose significant socio-economic impact and data security risks to retail companies where relatively little qualitative empirical studies have been done in the area of IIDTRC prevention.

Historically, IIDTRC incidents have continued to increase rapidly as business organisations migrate more into the digital realm. The trends in the e-commerce have opened the door for dishonest employees to steal Personal Identifiable Data (PID) within their companies. The operation principle of e-commerce, according to the Journal of Electronic Commerce Research, involves the sharing of business information, maintaining business relationships and conducting business transactions by means of telecommunications networks.

With the fourth industrial revolution, aka Industry 4.0, businesses are playing catch up with the increasing adoption of interconnectivity through the Internet of Things (IoT), automation, access to real-time data and Artificial Intelligence, which Industry 4.0 focuses on. This new phase of industrial revolution poses huge responsibility to business, their IT systems and IT security practitioners to ensure their data, especially PID, are processed in a secure manner. Shopon et al. (2022) noted that IIDTRC is one of the most common privacy invasions that can be done through leakage of multi-modal biometric information within business organisations.

✉ Romanus Izuchukwu Okeke
rokeke@cardiffmet.ac.uk

Max Hashem Eiza
M.HashemEiza@ljmu.ac.uk

[1] Cardiff School of Management, Cardiff Metropolitan University, Western Avenue, Cardiff CF5 2YB, UK

[2] School of Computer Science and Mathematics, Faculty of Engineering and Technology, Liverpool John Moores University, Byrom Street, Liverpool L3 3AF, UK

Published online: 01 September 2022

Organisation for Economic Cooperation and Development (OECD) (2008) defined IIDTRC as 'the unlawful manipulation' of information system (IS) by dishonest employees to steal PID. Identity Theft Resource Centre (ITRC) indicated that the incidents of IIDTRC continue to contribute to the number of breaches that affect millions of people. ITRC noted that in 2019 and 2020, threats that were internal and emerged from employees represent 15% and 20% of the total threats, respectively. IIDTRC incidents continue to increase across industries, for the past ten years, with three-fifth of retail industries suffered from these crimes compared to only one-sixth of technology (Potter & Waterfall, 2012).

Advancement of retail operations and increasing incidents of identity theft-related crimes create significant pressure on retail businesses to improve their security performance. The British Retail Consortium (BRC, 2019) found that the cost of fraud is up 5% to £163 million in 2019 in comparison to 2018 where insider and credit card fraud being the most difficult types to tackle. This report is based on a survey of UK retailers representing around one fifth of turn over turning over £103 billion, which is just under a third of the industry. Some of the loss figures have overlapped with cybersecurity attacks, theft of data and insider related crimes, which indicates that UK retailers are facing increasing lost revenue from identity theft-related crimes. The UK Cabinet Office estimates that digitisation of the retail industry and rapid growth in the use of credit and debit cards raises the need for understanding potential risks of IDTRC.

In 2015, the Centre for Retail Research indicated that the UK online retail was estimated at more than £52.4 billion industry which accounts for more than 5 per cent of the Gross Domestic Product and more than 10 per cent of all employment (Centre for Retail Research, 2015). This has been classified as one of the sectors where most consumers are vulnerable to identity theft related crimes with less investment on prevention. According to Crimestoppers UK, more than 20 organisations (excluding 30 top information security companies) have been dedicated to identity theft related crime prevention in the UK and other European countries; however, little has been achieved because of the lack of effective IIDTRC prevention.

There is an existing research gap in the areas of preventing IIDTRC. There is little literature on novel IIDTRC prevention strategies in a specific business context because of these crimes multi-faceted nature and interwoven modes of propagation, and ever adaptive nature. The existing IIDTRC prevention strategies were designed in the context of generic business organisations. Others were modelled to be implemented only on computer systems neglecting the importance of the cross functional management roles. Many available IIDTRC prevention models have little or no empirical research to ground their findings. Recent studies (Salam et al., 2021; Walsh et al., 2019) suggest that development of robust IIDTRC prevention strategy should be done in a clearly defined context – theoretical domain, geography, or business sector as well as critical examination of the management roles in handling of internal data security (Okeke & Shah, 2016). Others have focused on a methodological approach of using online games to simulate insider betrayal (Ho & Warkentin, 2017); and anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms (Mirza et al., 2014;), and a collaborative security approach to tackling internet security issues (Internet Security, 2015).

The purpose of this study is to contribute towards addressing the identified research gaps. It aims to examine challenges of preventing IIDTRC in the UK retails sector. This is achieved through two research objectives: 1) investigate the roles of cross-functional management team in prevention of IDTRC; and 2) analyse roles of cross functional management team in preventing IIDTRC in retail companies. We adopted in-depth qualitative multiple case studies to investigate the roles of cross-functional management team in preventing IIDTRC with focus to answer two research questions: 1) What are the roles of management team (crime prevention and data security) in preventing IIDTRC?; 2) What are the issues or challenges of preventing IIDTRC as an individual manager or management team for data security and crime prevention?

Our findings suggest that vagueness of roles and lack of clarity in sharing data security responsibilities are the major challenges of preventing IIDTRC among cross-functional management in the UK retail companies. To address the identified challenges, we suggest the application of RBF which provides a conceptual analysis using theoretical lens of organisational role theory (ORT). RBF model is deployed to analyse the collaboration of clear management roles with a specific focus on prevention of IIDTRC. RBF model synthesis the integration of both the external and internal environment for any adoption of IIDTRC preventive strategy, adoption of strategies to collaborate with cross-functional management and employees in preventing IIDTRC, and ensuring proper education and awareness among employees to prevent IIDTRC within organisations.

The rest of this section provides related research on the nature of IIDTRC, followed by the theoretical background of the RBF model. Section 2 covers the research method including data collection and analysis. The findings are discussed in Sect. 3, followed by the conclusion and future research directions in Sect. 4.

1.1 Historic Decades of Increasing Incidents and Impacts of Internal Identity Theft Related Crimes

Historically, the decade of 1990s marks an introduction of revolutionary era of an early online card processing services

– First Virtual, Cybercash, and Verisign. It was noted that approximately 62% of employees perpetrated IIDTRC in business organisation (Barling, 1995). Subsequently KPMG and Ernst & Young respective survey in 1997 and 1998 noted that IDTRC are often carried out by employees from shopfloor to the managements. Collins (2006) reported that 70% of IIDTRC are committed in the workplace by dishonest employees. It was also reported that out of 53% of 217 incidents of identity theft related crimes, 26.5% were originated from the business organisations (Romanosky et al., 2008). From the PWC's 2010 survey report, IIDTRC incidents had tripled compared to 2008. These and similar reports on the incidents of IIDTRC in business organisations has continued to appear in daily business media publications. In 2010, the Association of Certified Fraud Examiners (ACFE) indicated more than 80% of incidents of IIDTRC out of 1,900 cases of employees' fraud. It noted that 54% of these crimes were perpetrated by the business owners, executives, and managers. The increasing cases of these crimes pose socio-economic impacts and security risks. These issues have made the information security experts to carry a huge responsibility (Stickley, 2009). IBM Research noted that 73% of ICT employees fear losing their job in the case of IIDTRC incident (Chen & Rohatgi, 2008). The ACFE (2010) reported that a typical business organisation lost 5% of its annual revenue to IIDTRC. These crimes cost businesses about $221 billion annually excluding the psychological and legal costs, threats to the global security and damage to the reputation of the victims (Kroll, 2010).

The cost of IIDTRC is inestimable. It ranges from the reputational brand damage, costly customer account repair, information system failure of the victim industry to the psychological damages of the victimised consumers. The research by Experian Data Breach Resolution reported that it takes many years to restore company's reputation after a typical IIDTRC incident. They noted that the estimated minimum loss to their brand value was 12%. In some cases, companies face the wrath of the shareholders. Potter and Waterfall (2012) indicated a case of a company's stock price that fell by more than 70% following the reported IIDTRC incident. In today's age of social media, a single outburst of customer's PID theft could spread like a wildfire via social media. Sometimes the implication of these crimes leads to the folding up of the victim industry. For the past 10 years in the UK, the IIDTRC cost is placed at £3.2 billion with more than 70% incidents per annum. The survey placed UK retail industry as one of business sectors where IIDTRC incidents are prevalent (Kroll, 2011). The increasing IIDTRC incidents underwrite to more than 48.6% of retail loss and shrinkage (BRC, 2015). The elements of IIDTRC often involve compromise of consumers' PID and business commercial data through account identity fraud, account take-over, privacy counterfeiting and account withdrawal. Studies noted that the majority of consumers do not shop online because of their personal data security risks and lack of trust in its employees (Lyytinen & Grover, 2017; Zimmer et al., 2010), and noted that many consumers believed that retailers were primarily responsible for online transactions safety against identity theft and cyber-enabled crimes. Unfortunately, such consumers' perceptions still remain an irony.

1.2 The Nature of Internal Identity Theft Related Crimes in Business Organisations

Research has noted botnets, coercion, collaboration, collusion, infiltration, and social engineering as the common mechanisms of IIDTRC in retail companies (CIFAS, 2021), with IIDTRC and misuse of facility (and facility takeover) cases made up 82% of total cases recorded to the UK National Fraud Database. The UK Action Fraud explains that an account or facility takeover happens when a fraudster poses as a genuine customer, gains control of an account and then makes unauthorised transactions. An account can be taken over by dishonest or disgruntled employees and fraudsters, including bank, credit card, email, and other service providers. Dishonest employees can collaborate or collude with cyber-crooks to generate phishing pages for nearly any retail company around the globe at a click of a mouse or a tap of a keyboard. In some cases, the criminal could infiltrate a company for the sole mission of committing IIDTRC.

Researchers (e.g., Wakunuma & Stahl, 2014) have noted that at times, honest employees face increasing challenges of external pressure through coercion luring them to compromise their professional work ethics and commit IIDTRC. Luo et al. (2020) developed a comprehensive model of employee-committed malicious computer abuse to indicate the effects of the individual characteristics of self-control, hacking self-efficacy, moral beliefs, and the effect of security guardianship in organisational settings. Their model shows how certain circumstances can lead an employee to commit a malicious their organisation.

Huth et al. (2013) noted that the challenges of preventing, detecting, and responding to data leakage propagated by authorised users, or insider threats, are among the most difficult issues facing security researchers and professionals today. Researchers in the quest for the IIDTRC prevention often asked; why have available IIDTRC frameworks failed to prevent the crimes? Some research answers attributed the failure to poor understanding of the nature of IIDTRC by crime prevention management and lack of clear responsibilities given on internal data security (Shah & Okeke, 2011; Okeke & Shah, 2016). These challenges have left business managers with little or no better option than to resort to generic IIDTRC prevention models.

1.3 Generic Prevention Model and Software Security are not Enough

Till date, specific literature on prevention of IIDTRC is scarce and the existing IIDTRC prevention models focus on the implementation of software security and data protection policies. This is due to challenges in managing the chains of roles required for prevention of these crimes in retail industries. For instance, most outsourcing firms run into difficulty in offering an identity monitoring service for their customers. This is due to the fact that some employees within the business organisations thwart credit-monitoring processes. Moreover, security technologies and policies become useless when employees misunderstand or deliberately ignore information security policies in the organisation turning from compliant to non-compliant employees (Chen et al., 2021) owing to the stipulations that the outsourcing firms are not part of their statutory data protection policy. Such circumstances contribute to the identity monitoring service delays which often caused the reports to arrive days after the IIDTRC incidents have transpired. Researchers have also attributed the scarcity of the literature to various reasons including the attitudes of legal entities and business owners and security professionals. Guéraiche (2022) noted that some data privacy regulations prohibit sharing of IIDTRC prevention strategies across business organisations, although countries, communities, and citizens, and allows information sharing across the globe, and this attitude restricts investigations which may help future prevention of similar IIDTRC. Data security professional are often unwilling to share their security strategies and solutions (Biglari & Pourabedin, 2022), which they treat as, sometimes, a way of gaining competitive advantage.

The ACFE noted that more research is required to be conducted in the context of a particular business organisation with focus on an in-depth understanding of the roles of cross functional management team in preventing IIDTRC. Stalla-Bourdillon (2014) emphasised the need for in-depth understanding of the management roles and their implications in business information system security. Okeke (2015) suggests that studying the management implication is a vital prerequisite for modelling effective IIDTRC prevention strategies, which requires integration of role-based strategies which includes IT security and crime prevention team would enhance prevention IIDTRC crimes.

Other studies (e.g., Cross & Layt, 2021; Wyre et al., 2020) noted that the collaborative effort of 'human resource security' – management team and law enforcement agency, are often overlooked in formulation of IIDTRC prevention strategies. They emphasised the need to collaborate with these actors, since these crimes prevention are often complicated with many internal and external influences. They also noted that clear guidance on management roles in IIDTRC prevention strategies are key issues that required further research exploration. Shah and Cross and Layt (2021) agrees with Okeke and Shah (2016) that some data security management strategies failed to prevent these crimes because they do not incorporate the external management roles. They further suggested that IIDTRC prevention frameworks should have both theoretical and empirical underpinnings from the perspectives of the organisation under study. In this work, we will address these suggestions by using the theoretical concept of RBF model to study the prevention of IIDTRC in retail companies, to help analyse cross-functional roles of the management and their deployment of the IIDTRC prevention strategies.

1.4 Theoretical Concept of Role-Based Framework

Role-Based Framework (RBF) is a concept which devolves the collaboration of shared roles to managements involved in prevention of IIDTRC. The synthesis of RBF is based on the proposition that the effectiveness of IIDTRC preventive frameworks is dependent on the clarity of the shared roles of the crime prevention managements. Therefore, effectiveness is dependent on the clarity of shared roles the managements uphold. To analyse RBF, we applied the concept of organisational role theory (ORT) – the manner in which individuals accept and enact an array of roles in task-oriented and hierarchical systems. Mertens (2003) noted that building empirical grounded theory, as it is in this study, requires a reciprocal relationship between data and theory. Applying this concept in this study, we generated the framework based on the *a priori* models and then used ORT as a theoretical lens to guide the study. Ekblom (2010) suggested that though know-how-knowledge of the process of the crime prevention plays a central role for implementation of framework for any sort of crimes, the success depends on understanding the organisational structure of the context under study. Other researchers noted that the analysis of interaction between the crime prevention management and their immediate environment starts with understanding both entities as institutional configuration in the same socioeconomic setting; how they cohabit side by side with utmost aim of greater efficiency and productivity (Lawrence et al., 2009). Hodgson (2006) also suggested 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 ORT to explore these relationships, since roles in the context of hierarchical (as shown in Fig. 1) management system like retail industry are not defined in isolation but in a 'social or organisational net of role relationships' (Cabri et al., 2006).

ORT is premised on the notion of the manner in which management enacts the arrays of roles (shared roles) in the

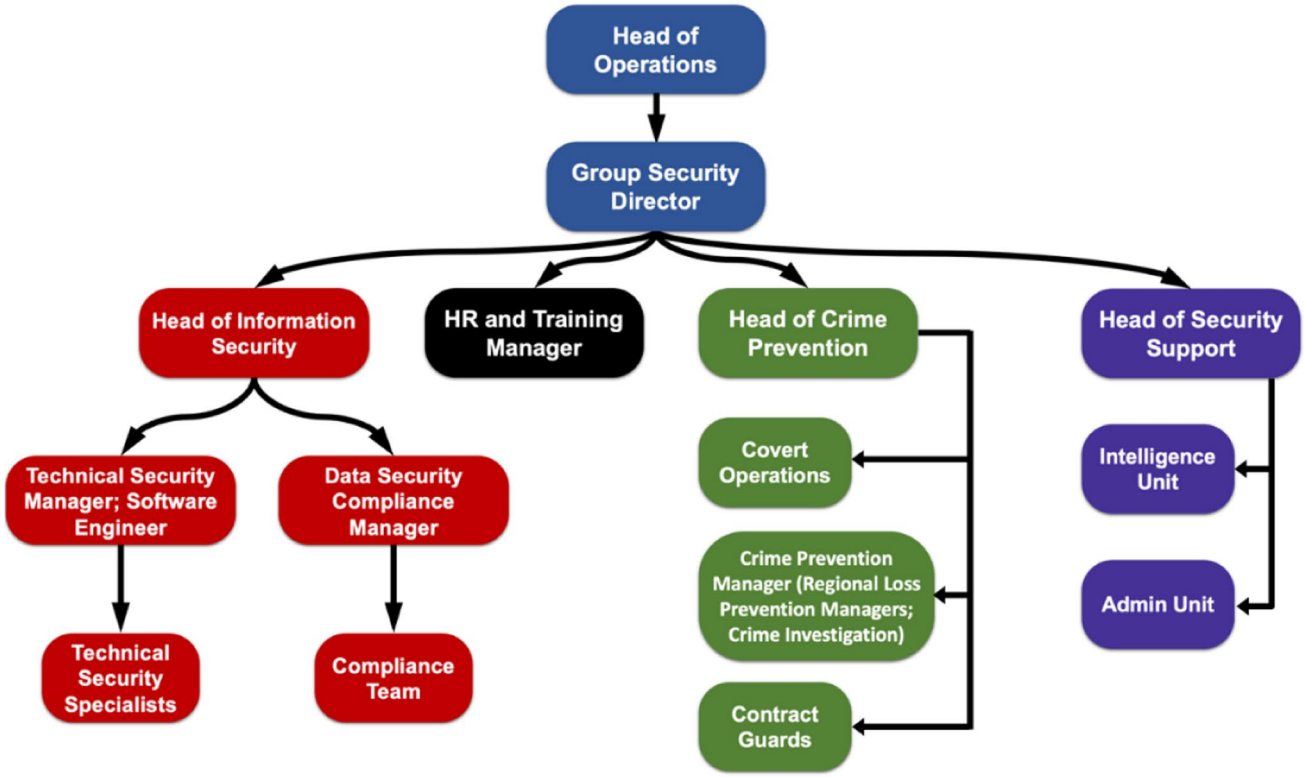

Fig. 1 Hierarchical order of the internal data security and crime prevention management

task oriented hierarchical systems (retail industry). It focuses on effective functioning of the roles within the organisation, and the interaction between roles and the impact this has on achieving organisational goals (Biddle, 1986; Katz & Kahn, 1966; Madsen, 2002). The concept of ORT, developed in the 1960s, provides insight into the purposive actions of individual employees, managements, and organisations, as they relate to the system in which they operate (Kahn & Katz, 1978). ORT concepts have been applied widely in behavioural science, management, sociology, and psychology. It has been used by many studies in modelling the authority, responsibility, functions, and interactions associated with management positions in business organisations (Shah & Clarke, 2009; Zhang & Yin, 2006).

In their extensive study of how organisations can prevent crimes in their respective business domain, Ekblom (2010) and Sarnecki (2005) adopted the idea of ORT and suggested that management in the organisations must in some way complement the shared roles and responsibilities; support each other in the environment where they operate. Biegelman (2009) also asserts that all the roles, including those of the complementary entities depends on each other to thrive in crime prevention within any business organisations. Luhmann (2004) in support of these suggestions noted that a deeper understanding of implications of management roles in business organisation is an important prerequisite in modelling a robust IIDTRC prevention. The interdependency of management roles as articulated by Ekblom (2010) and Sarnecki (2005), creates the basis of analysis of '*shared roles'* among the crime prevention management in this study. The ensuing interaction becomes a role-based process where each party begins to share roles of each other, with clarity of valued interest of effective IIDTRC prevention.

To analyse the structure, processes, and operationalisation of these relationships between various roles of human resources involve in crime prevention management, a role-based framework is adopted. Based on the assumptions of the Ekblom (2010), Zhang and Yin (2006), Sarnecki (2005), and Kahn and Katz (1978), the application 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 roles of cross-functional management team and the implication of their interaction with other managements (IT security, data compliance, law enforcement agencies) and how it can help to minimise employees indulgent in IIDTRC,
- to help explain the impact of the clarity of crime prevention management roles and how it can help to maximise managements performance in providing effective internal data security.

Table 1 Semi-structured interview participant's management position

	Role	Management Position	Base CIC Plc firm	Mode of interview
P1	IT Security	Head of security support	CIC Plc	Face-to-face
P2	Crimes Prevention	Head of crimes investigation	CIC Plc	Face-to-face
P3	Data Compliance	Group Data Compliance manager	CIC Plc	Face-to-face
P4	Crimes prevention	Head of Crimes prevention	CIC Plc	Face-to-face
P5	Operations	Head of Security of Operations	CIC Plc	Face-to-face
P6	IT Security	Technical security support	XGroup	Telephone
P7	Human Resources	Training Manager	ZGroup	Face-to-face
P8	IT Security	Software Engineer	ZGroup	Face-to-face
P9	IT Security	Compliance team manager	YGroup	Telephone
P10	IT security	Technical Security Specialist	YGroup	Telephone
P11	Crimes prevention	Regional Loss Prevention manager	XGroup	Face-to-face
P12	Human Resources	Head of Human Resources	CIC Plc	Face-to-face

Total number of participants from each of the selected firm = 12; CIC Plc = 6; XGroup = 2; YGroup = 2; ZGroup = 2

2 Research Methodology

On exploring the assumptions made in the above sections, this study adopted a qualitative case study which enabled us to gain familiarity with the problem and generate new insights (Bryman, 2001; Eisenhardt, 1989). The qualitative case study is applied in this case to enable a complex phenomenon to be explored through the identification and analysis of different factors, including roles of cross-functional management team interacting with each other. We conducted face-to-face semi-structured interviews which involved 12 top security and crime prevention managers selected from the four participating firms. Table 1 below shows their respective roles, management positions, and mode of interview. They were interviewed on the issues related to their roles and the challenges they encounter in handling internal data security and IIDTRC prevention.

2.1 Research Setting: Case Study of CIC Plc

This case study was carried out on retail firms in the UK. The group of retail firms – CIC Plc. (the name of the firm have been changed for the sake of confidentiality); is a successful retail corporation in the UK. In total, four retail firms: CIC Plc, including XGroup, YGroup and ZGroup which make up CIC Plc. 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 (Yin, 1984). Secondly, these firms' business culture and ethics, and their experiences in e-tailing are recognised as the common operation the retail industry across UK adopts. CIC Plc. has over 13 million employees that handle more than 15 million customers' data and over 30 million calls per day. In the mid-2000, CIC Plc. extended their operation from financial to sourcing services. The extended services enabled them to offer millions of customers a variety of products such as credit, extended warranty, and insurance products. Thirdly, CIC Plc. Group were willing facilitators and participants in this research. They provided the data required—a key practical consideration when embarking on field-based research (Pettigrew, 1990).

For the fieldwork, we chose their three branch offices in the north-west of the UK which are closer to the researchers' base-university. Although these three branches are part of the CIC Plc, each of the branches retains their business operations and distinct brand names as XGroup, YGroup and ZGroup respectively. All the selected participants from the three distinct brands have worked for RGroup for at least five years, and have led in developing and implementing IIDTRC prevention strategies in CIC Plc. In total six participants were based in the CIC Plc, as shown in Table 1.

2.2 Rationale for XGroup, YGroup and ZGroup

XGroup This is one of the largest retail firms, incorporated as part of RGroup in the UK and operates in many regions across the country with the trend in retail business operations (trading of trending products such as are grocery, clothing, and home wares). It employs over hundreds of staff in the UK and handles millions of customers' data coming through thousands of online orders per annum as well as financial services such as credit and extended warranty services. Table 1 indicates that two participants were selected from this XGroup.

YGroup Similarly, YGroup, part of RGroup Plc, is one of the top 20 UK retail companies with a multi-million pounds worth of annual revenue. Specialising in financial services and household items, it boasts of hundreds of employees

who transacts millions of customers' data personal identifiable data via e-commerce platforms per week either online or over the phone. Table 1 depicts that two participants are based in YGroup.

ZGroup This third retail firm has a similar business operation with both XGroup and YGroup. Although with less annual income comparatively, it handles thousands of the customers' personal data. Two participants were, as shown Table 1, were selected from ZGroup.

Collectively these retail firms, as part of CIC Plc. have extended retail business operations including data services and e-business servicing and outsourcing as well as mail order trading via catalogues and websites. Other financial services include fraud prevention and operational risk.

As this research is centred on the IT security and crime prevention managements, the choice of the location enabled us to get access to data environment and see security resources with ease, on time and at reduced costs (Hakim, 2000). The key role of these managements is to ensure that CIC Plc. retailing operation comply with the UK Financial Services Authority. They are committed to protect customers' data and prevent data theft and leakages.

Figure 1 above shows the hierarchical order of the management team headed by the group security director who reports to the head of operations. Group security director is responsible for integration of security operations – IT security, HR, and security support. Next is the head of information security who oversees other security operations – technical and compliance. The head of security support is responsible for the intelligence unit and administration. The head of crime prevention is responsible for crime related operations – detection, investigation, etc. CIC Plc. also outsources to renowned IT security companies such as IBM and RSA.

2.3 Data Collection and Analysis

Each interview session lasted for a maximum of 1 h 30 min. In several cases, multiple interviews were conducted, and notable issues were compared for consistency and validity (Yin, 1984). While conducting the interviews, a technique of 'theoretical sampling' was adopted (Strauss & Corbin, 1998). If a set of factors and parameters that led to a certain outcome were identified, the enquiries would be directed to determine the change in the outcome. This strategy helped to ascertain a better understanding of the causes of the IIDTRC incidents. For instance, we investigated whether the observed cause of a certain incidents was due to employees not adhering to the data security policy. In this manner, we investigated whether the incidents had occurred due to the security policy related issues, or it was due to the unique software security loopholes. We also used IIDTRC case reports to supplement the interview data.

2.3.1 Semi-Structured Interview Questions

The researchers set out guiding questions underpinned by the research question: what are the roles of cross-functional management team in preventing IIDTRC? The guiding questions enabled researchers to ensure that research questions are aligned with the RBF attributes – which focus on explaining the roles of cross-functional management team and the implication of their interaction with other managements. The guiding questions are:

1) *What are your (P1, P2, P3, …,* etc.*) roles/ responsibilities as part of the management team in preventing IIDTRC?*
2) *What are your (P1, P2, P3, …,* etc.*) challenges of prevention IIDTRC as an individual or team in your business (CIC Plc, XGroup, YGroup, ZGroup)?*
3) *What data security issues do you (P1, P2, P3, …,* etc.*) encounter in preventing IIDTRC as an individual or as a team?*

These guiding questions were used to explore company's issues involving the nature of IIDTRC prevention extending 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. These research questions were used as the topic guide for the enquiry.

2.3.2 Development of Codebook

The recorded interviews were transcribed selectively and coded. We deployed Nvivo to enable data collation process to provide a minimally (e.g. transcripts) to maximally (e.g. open-ended questions) structured codes. We collated corpus of transcribed interviews and coded the text index according to specific research questions (used to frame the interviews). For instance, 'Q1. What are your (P1, P2, P3, …, etc.) roles as part of the management team in preventing IIDTRC?' was coded as 'roles and responsibilities as part of IIDTRC prevention team'; the 'Q2. What are your (P1, P2, P3,…, etc.) challenges of prevention IIDTRC as an individual or team in your business (CIC Plc, XGroup, YGroup, ZGroup)?' was coded as 'challenges of preventing IIDTRC as an individual or a team; and the 'Q3. What data security issues do you (P1, P2, P3,…, etc.) encounter in preventing IIDTRC as an individual or as a team?' was coded as 'data security issues in preventing IIDTRC as an individual or a team'.

In developing the codes, we adhered to the suggestion of Bernard (1994) and MacQueen et al. (1998) that codes can

be used for indexing or measurement. Hence we focused on using index codes generated from the Nvivo to tag text from the interview transcripts. This approach enabled ease for retrieval and measurement of codes and to assign meaningful values to text such as frequency and amount/count of codes as well as either presence or absence of the information (Bernard, 1994).

As shown in Table 2 the presence of information is denoted by '1' and absence by '0'. The total number of presence of codes were aggregated across the parent codes. In quantifying the presence of the information, the codes were use to add information to the text, rather than reducing the text, which agrees with interpretative underpinning of this study while allowing for simultaneous break down of texts into meaningful segments.

We labelled the text index as structural coding which enabled us to facilitate subsequent analysis and then identified all the texts associate with each of the research questions. We applied structural coding to identify and analyse texts that are out of sequence with original interview structure; thus, generating aggregate codes. This approach allowed us to manage situations where the participants spontaneously digress from research questions, which is what MacQueen et al. (1998) termed 'cognitive leap'. Our goal was to code the texts into meanings and format that is reliable and verifiable using quantitative database.

For instance, Table 2 presents a matrix for group of responses to the research questions concerning 'challenges of managing IIDTRC' regarding 'IIDTRC_MGT_ISSUES = Management Roles Related Issues' and 'DATASEC_ISSUES = Data Security Issues'. Using the matrix it was possible for us to attach values to the codes. Hence, we could quantify the total number of presence of parent codes from each of the participant's responses. And the parent codes are labelled across the columns: 'INDIV_DATASEC_CHAL = data security challenge of an individual role'; 'TEAM_DATASEC_CHAL = data security challenges of a team role'; 'INDIV_PERC = respondent perceives IIDTRC as individual issues/challenges'; and 'TEAM_PERC = respondent perceives IIDTRC as team issues/challenges'; whereas the corresponding participant's responses are labelled with '0 s' and '1 s' across the rows.

We used codes to primarily signal the presence or absence of meaningful pieces of information. The responses labelled with '0 s' and '1 s' matrix for 'absence' and 'presence' respectively were counted to get the total number of presence of each of the parent codes, as shown in Fig. 2.

The matrix enabled us to quantitatively analyse open-ended responses while limiting the total number of codes elicited. Figure 2 shows total number of presence of parent codes, with 'IIDTRC_MGT_ISSUES = Management Roles Related Issues' equals 'TEAM_PERC = respondent perceives IIDTRC as team issues/challenges'. This equality shows agreement between the perceptions of participants and coded parents codes. However, the total number of presence of parent codes regarding 'TEAM_DATASEC_CHAL = data security challenges of a team role' is less than the number of presence of 'TEAM_DATASEC_CHAL = data security challenges of a team role'. Overall, the matrix shows the overlap of codes across the parent codes as shown in Table 2 which is reflected in the structure of Figs. 3 and 4 below.

2.3.3 Reliability Score of the Coding

We employed 'testing and refining the codebook' process recommended by MacQueen et al. (1998), as shown in Fig. 3. We had a number of meetings to plan and agree on coding process as well as to evaluate use of proposed code list and coder's ability to use and apply the codes in a verifiable and consistent manager. We started with development of the initial code list, which was modified as we progressed with coding independently. With the use of Nvivo the modification was monitored and we had meeting to discuss any changes. Where the changes are acceptable and consistent, we continue to code. However, where the change are inconsistent and disagreed, the codebook was reviewed and revised and then recoded. This process was cyclical around either direction of 'acceptable and consistent' and 'unacceptable and inconsistent', as shown in Fig. 3. For instance, some inconsistencies were linked with the code definitions such as use of ambiguous inclusion criteria that make it difficult to differentiate between to parent codes.

2.3.4 Percent Agreement and Cohen's Kappa Coefficient of the Codes

In addition, we used Coding Comparison Query on Nvivo to compare parent codes, and to measure inter-rater reliability which is the degree of coding agreement between two or more users. The use of Nvivo's Coding Comparison Query enabled us to measure coding agreement using Percent Agreement and Cohen's Kappa Coefficient (K) of the former is the number of content units on which coders agree (to code or not to code), divided by the total number of units—reported as a percentage, and latter is a statistical measure that takes into account the amount of agreement expected by chance—expressed as a decimal in the range –1 to 1 (where values ≤ 0 indicate no agreement, and 1 indicates perfect agreement) (Nvivo 12, n.d).

Table 3 depicts that average coding agreement rating regarding the parent codes is 90.82% while average disagreement coding is 9.18%. Various authors (e.g. Falotico & Quatto, 2015; McHugh, 2012; Xie, 2013) have suggested different guideline for interpreting K and Percent Agreement. Specifically Xie (2013) indicated that K with values between 0.75 to 1.0 is a 'very good strength of agreement'

Table 2 Codebook for parent codes

Participant ID	RESPONSE	Parent Codes (to signal the presence or absence of particular pieces of information)					
		MGT_ ISSUES	DATASEC_ ISSUES	INDIV_DATA-SEC_CHAL	TEAM_DATA-SEC_CHAL	INDIV_PERC	TEAM_PERC
P1	We have very good relationship with the police…, with my twelve years of experience of working 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 retail businesses	1	0	0	1	0	1
	Well, these security tools are not cheap, and we are talking about CIC Plc of many branches spread across UK…., besides, the security companies never stop designing new product…, we cannot go beyond the company's budget	0	1	0	0	1	0
	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 CIC Plc; they utilize the resources they have at their disposal to implement the latest security tool for prevention of the IIDTRC challenges in the prevention of IIDTRC in the CIC Plc include the budget constraints, the employees' expertise, and pace of the evolving digital security technologies	0	1	0	0	1	0
P2	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	1	0	0	0	1	0
	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 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 take lots of times and expertise. Besides we need to hire professionals to do that	1	1	0	1	0	1
	CIC Plc were busy with their routine of IIDTRC escalation process; detection, investigation	1	0	0	0	0	1
	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	1	0	1	1	1	1
	CIC Plc 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 has an influence on the amount of effort the law enforcement agency/police input in IIDTRC investigation	1	0	0	0	0	1
	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'	1	0	0	0	0	1
	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'						

Table 2 (continued)

Participant ID	RESPONSE	Parent Codes (to signal the presence or absence of particular pieces of information)					
		MGT_ ISSUES	DATASEC_ ISSUES	INDIV_DATA-SEC_CHAL	TEAM_DATA-SEC_CHAL	INDIV_PERC	TEAM_PERC
P3	We have just revoked a contract with one of outsourcing companies because of their laxity in abiding by our stipulated data security measures…We requested for the printout of all network security test updates of which they provided. We found out that some of the test that was not successful, we then asked to update that and resend the results….but they failed to implement our request. We have no other option than to revoke the contract	0	1	0	1	1	1
	Most of these agencies' managements do not have good knowledge of data security expertise in carrying out their responsibilities in prevention of the IIDTRC as compared to what is obtainable in this organisation…	1	1	0	0	1	0
	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	0	1	0	1	1	0
	It often delays investigation protocols because of roles clarifications such as 'who does what and where do we go first' in handling internal data security breaches	1	1	1	0	1	1
P4	Sometimes managements often allow issues such as the 'seriousness' of the crime, perceptions, culture, and outcome of a crime incident, to interfere with their security strategies	1	1	0	1	0	1
	the firms still treat IIDTRC prevention policy as 'their business	1	0	0	0	0	1
P5	CIC Plc 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	1	1	0	1	0	1
P6	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	0	0	0	0	1	1
P7	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 change and start switching their roles	1	1	0	0	1	0
P8	I'd always continue with my major job roles, which is basically designing of 'ZGroup' secured systems applications, when the need for computer crimes issue comes up, the management handles those…	1	0	0	0	0	1
	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…	0	0	0	0	1	0
P9	When 'CIC Plc' 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	0	1	0	1	0	1

Table 2 (continued)

Participant ID	RESPONSE	Parent Codes (to signal the presence or absence of particular pieces of information)					
		MGT_ ISSUES	DATASEC_ ISSUES	INDIV_DATA-SEC_CHAL	TEAM_DATA-SEC_CHAL	INDIV_PERC	TEAM_PERC
P10	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	1	1	0	1	0	1
	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	0	1	0	0	1	0
	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. This issue has led these complimentary management team to place a lot of emphasis on abiding by the data security policies of CIC Plc but neglecting the key aspect of IT security which internal security control	1	1	0	1	0	1
	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	1	0	0	1	0	1
P11	some of the crimes prevention or intervention failed because of inadequate resources – money and security experts; 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	1	1	0	1	0	1
P12	We have to ensure that our employees are trained and are updated on data protection policy; or are conversant of the consequences of data security violation. My management team in this organisation take these steps as our responsibility. We have designed a comprehensive training programme for the employees across security management – physical security staff, surveillance, software engineers, on criminal law course. 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	1	1	0	1	0	1
	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	1	1	0	1	1	1
	Total number of presence of parent codes	**20**	**17**	**2**	**14**	**13**	**20**

whereas values between 0.00 to 0.075 is 'slight strength of agreement'. Similarly, McHugh (2012) noted that Percent Agreement with values between 82 to 90% is almost perfect. Drawing from both Xie (2013) and McHugh (2012) indications, the reliability score of our coding is 'almost perfect' rating for the Percent Agreement whereas some codes 'very good strength of agreement' with some 'slight strength of agreement'.

2.3.5 Thematic Coding

As suggested by Carley (1993), the process of coding is one of the selective reductions which help to reduce the texts into categories of phrases. In this case, coding enabled us to focus on phrases that are indicative of the research questions and objectives. Based on concept of content analysis suggested by Weber (1990), 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 sort out the real owner of particular identity data details was coded 'IIDTRC incidents and intervention outcomes'. Such issues are broadly categorised under 'segregated data security policies'. Similarly, 'structure of IIDTRC prevention strategy' are coded within the 'Management roles related issues' category. We also eliminated each of the subcategories that did not result in 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 managements, we did consider this incident (though indirectly related) as a relevant issue to this study.

The phrases in subcategories indicated the notable issues and challenges. Since each of the subcategories featured multiple issues, they represented potential IIDTRC prevention issues which arise in retail industry but were not specific to any single IIDTRC incident. Hence, using the process of systematic open-ended questions, coding across participants at various management positions, and by comparing their anecdotes and generated codes, we were able to arrive at a preliminary model of some of the key internal data security challenges of management on prevention of the IIDTRC in the UK retail industry. The model below shows the two main categories and respective subcategories. Each of these coding categories and their interrelationships with their subcategories are shown in Fig. 4.

2.3.6 Management Roles Related Issues

The managements in our case study seem to have good knowledge of their roles and responsibilities in handling internal data security and IIDTRC prevention. The challenging issue is that they lack effective communications and role sharing with other complementary management such as law enforcement agencies and outsourcing companies. Several managers noted lax attitudes of the outsourcing and law enforcement managements as their major setback. The group data compliance manager in her response decried that:

> "Most of these agencies' managements do not have good knowledge of data security nor expertise in carrying out their responsibilities in prevention of the IIDTRC as compared to what is obtainable in this organisation…." It often delays investigation protocols because of roles clarifications such as 'who does what and where do we go first in handling internal data security breaches'.

Some outsourcing companies that are contracted to store customers' data often do not adhere to the data security management procedures.

Some of the third-party companies rarely '*buy in*' or adhere to the stipulated data security agreement. They handle internal data security loosely. 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 our organisation 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 lots of 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!"

Although there is contractual policy binding the retail organisation and outsourcing firms, they still treat IIDTRC prevention policy as 'it is their business (retail industry)'.

To put checks on these pervasive attitudes of the outsourcing companies, the data compliance management have resorted to coercion and thorough data security auditing. If both strategies failed, the organisation would revoke their business contract. The organisation's group data compliance manager described a recent experience:

> "We have just revoked a contract with one of outsourcing companies because of their laxity in abiding by our stipulated data security measures…We requested for the printout 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 to update that and resend the results…. but they failed to implement our request. We have no other option than to revoke the contract!"

Another major challenge in handling IIDTRC prevention is the lack of continuity in the roles of the law enforcement agency management. The head of crime investigation bemoaned the difficulty his team faces in trying to build effective working relationship with the local law

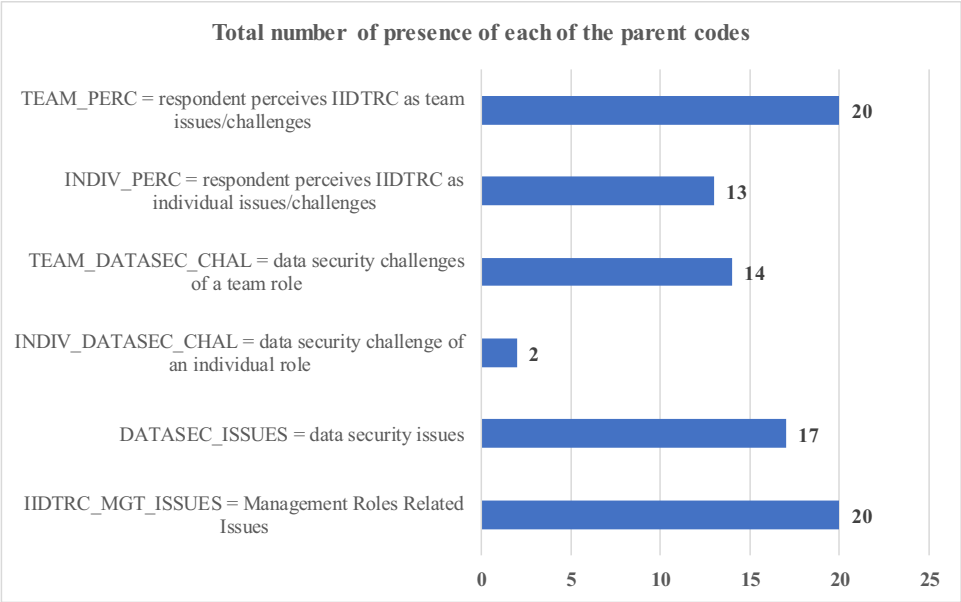

Fig. 2 Total number of presence of each of the parent codes

enforcement agency. He noted that this issue often led to delays during investigation of crimes:

> "When there is a change of the head of local area police, all the long-built relationship and working team would breakdown…, to build up 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……"

Moreover, there is an issue of varying views on data security and IIDTRC prevention among employees. It was observed that top managements and shop-floor management have different perception of data security and regulations. The shop-floor managers see internal data security regulations as the business of the top management alone. Much to the disappointment of the crime prevention management, however, their attempts to educate all the employees have not yielded expected result. This is due to the associated 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. To tackle this problem, they have introduced mandatory e-learning (data protection policy and regulations) and criminal law courses. It was designed to meet the educational requirements and levels of all management and employees.

The head of human resources noted:

> "We have to ensure that our employees are trained and are updated on data protection policy; or are conversant of the consequences of data security violation. My management team in this organisation take these steps as our responsibility. We have designed a comprehensive training programme for the employees across security management – physical security staff, surveillance, software engineers, on criminal law course. 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 IT Security Support 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…"

The management believe that there is need to invest on human resource development. This collective data security training campaign across the top managements are to ensure that employee would abide by the data security policies and stipulations.

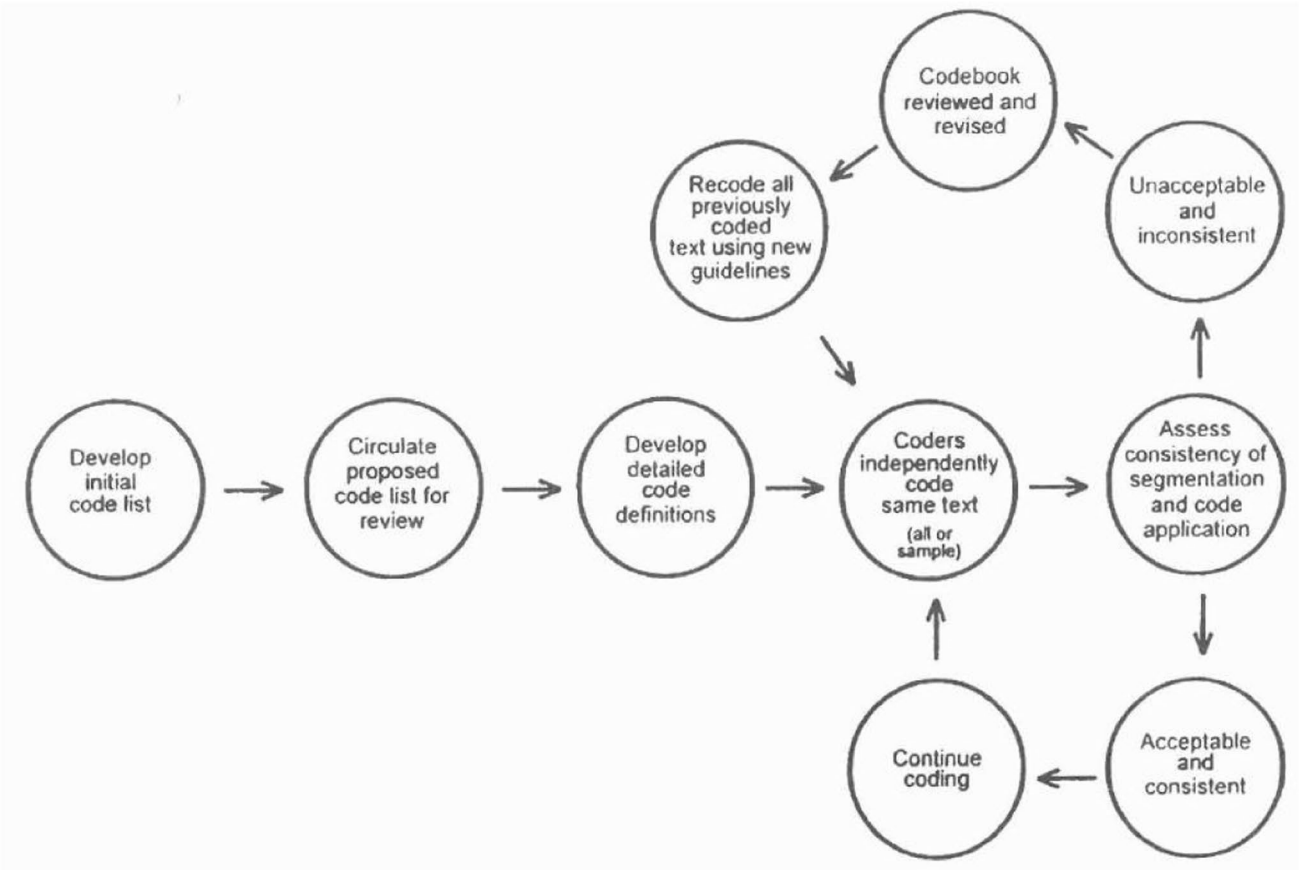

Fig. 3 Process of testing and refining the codebook (adapted, MacQueen et al. (1998))

2.3.7 Perceptions of Data Security Issues

Another key challenge in prevention of IIDTRC is different strategic approach adopted by management in handling IIDTRC incidents. The Head of Crimes prevention stated that;

> "Sometimes managements often allow issues such as the 'seriousness' of the crime, perceptions, culture, and outcome of a crime incident, to interfere with their security strategies".

On the issue of incident assessment and interventions, the managements seem to be somewhat 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 crimes investigation 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 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 take lots of times and expertise. Besides we need to hire professionals to do that."

This shows that some of the crimes preventions or intervention strategy failed because of the management perceptions.

Another challenge related to the perception of data security challenges is the assessment of successful and unsuccessful intervention. It is difficult for the security management to assess their successful IIDTRC prevention since the impact of these crimes differs on both the victims and businesses. The Head of Security of Operations 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 the Head of Security of Operations statement that

> "CIC Plc 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 is 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"

Similarly, there are cases where security loopholes were discovered within the IT platform. They were neglected because the organisation 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 data security.

Moreover, the cultural perception also influences the management roles in prevention. There is a culture of complacency among the security management where they continue with business as usual with reluctancy to change and adapt to the evolving IIDTRC, and this perception can weaken the security strategies in preventing IIDTRC. This is evidenced by the comment of the Training Manager;

"We are extraordinarily well-organised security management team, and every member of our management teamwork 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 change and start switching their roles".

This comment agrees with an observation from 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 'ZGroup' secured systems applications, when the need for computer crimes issue comes up, the management handles those…"

Similarly, the cultural perception of disregarding crime report from smaller cities or small business sectors influences decisions of the security management and law enforcement agencies in preventing IIDTRC in the retail companies. In response to the question of 'what is the attitude of the police in assisting the CIC Plc in mitigating IIDTRC', the Head of security support noted;

"We have very good relationship with the police…, with my twelve years of experience of working with 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 retail businesses."

In some cases, some of the IIDTRC are left to the point of escalation because the suspect is from a 'developed' country. Some of the crime prevention team seemed to believe that employees from the 'developing' or 'less developed' countries pose more security risks to the organisation than those from developed countries. The Regional Loss Prevention Manager remarked:

"Most crimes incidents we have observed are always employees from the 'minority ethnic groups'. Though sometimes there are bad ones from this country, but their cases are not 'that bad' compared to that of those from those 'minorities'."

This remark is in line with recent research targeting employees' groups rather than individuals to understand how these groups formulate their collective security efficacy, which impacts on how individual recognise and respond to security incidents (Johnston et al., 2019). In the same vein, there are areas within the UK where crimes are believed to be more prevalent than others. Most crimes incidents reports from cities such as London, Birmingham, Manchester, and Glasgow are always seen as cities of notoriety for these crimes. This belief in some cases are misconceptions, which often lead to negligence on the part of management's efforts in prevention of IIDTRC in retail industry.

3 Discussion

While CIC Plc. case analysis was not extreme, the categories summarised above cannot be considered a complete representative of crime prevention management challenges and issues. However, it shows that management of the outsourcing companies do not take data security and prevention of IIDTRC as their key responsibility. Besides, there are insufficient trained law enforcement agents with clear roles on how to handle IIDTRC in designated business organisations like retail industry. There is also the issue of varying understanding of data security related issues across the levels of employees. There are various security strategies attributed to the nature of the crimes, the environment of the crimes and cultural orientation of the perpetrators, which were not clearly coordinated. On the other hand, this case study suggested that training of employees is very difficult to achieve in retail industry due to the time and cost associated implications. Few retail industries may have incentives to invest significant resources in training their IT security and crimes prevention employees. As a result, they continue to adopt coercive data security strategy approaches which pay off on short term basis. However, the purpose of this case study was not to unveil a complete list of IIDTRC prevention challenges and issues in retail industry. This study was limited to the context of the UK retail industry. Therefore, the findings would not be extended to the nuances that would arise outside this context. Also, the case selection was restricted

to a group of retail organisations that share similar business operations and management culture. Therefore, the findings cannot be overgeneralised to all retail industries. The case study is used to explore and generate some significant case examples and attempt to find a suitable conceptual framework that would analyse these issues. Hence, next section introduces the concepts of role-based framework as a model that analyses the observed issues and challenges.

3.1 The Structure of Role-Based Framework

Role-Based Framework (RBF) is a role clarification concept designed to assist managements to improve their performance, by assisting them to select and replicate practices appropriate to their needs and circumstances. RBF was developed based on IIDTRC' prevention models which focus on the recommended principles management in crime preventions (Shah & Okeke, 2011). RBF conceptualises managements as the body that encompasses all the cross-functional team members – crime prevention, IT security, human resources, and law enforcement agency. It classifies management's roles in a hierarchical level from the top management to the front-line management (as depicted in Fig. 1). It also follows the stages of preventive processes which include intelligence, intervention, involvement, collaboration, and remediation measures.

RBF is organised as a sequence of management's levels which emphasise the clarification of roles – managements responsibilities, interactions, and interdependent roles. The arrows depict the interdependency of shared roles through monitoring, reporting, and collaboration across management's levels as shown in Fig. 5.

From the top managements, the RBF emphasises the importance of a clear IIDTRC prevention policy within any retail organisation. It is a necessary first step towards the effective IIDTRC prevention. There should be policy guidelines, clear procedures and internal rules for reporting and investigating cases of IIDTRC. Researchers suggested that good and clear data protection and information privacy policy statements are the basis for the scope of other steps to be built upon (Lyytinen & Grover, 2017). They suggested that a clear policy structure is the bedrock of IIDTRC prevention models. Okeke and Shah (2016) and Amasiatu and Shah (2018) emphasised the importance of effective data security policy that it should be defined with 'definitive objectives' in the areas of proper policy, monitoring, collaboration and reporting, without which the cross functional management team would not be effective. They suggested that a typical IIDTRC prevention policy should include data protection policy, crime prevention policy, deterrence policy, internal reporting policy.

The middle level management are accountable to the top-level management. They should be able to clarify and explain IIDTRC preventive and deterrent policies to lower-level management thus acting as a mediator between the two levels. The front-line management have a strong influence on the employees as they interact with them on a daily basis. They can play a vital role in the detection and investigation of incidents of IIDTRC. One of the most effective ways to mitigate the threat of IIDTRC such as collusion and coercion is to raise the awareness among all employees. Organisations via complementary management (human resources) need to ensure that the members of staff are aware of whom to report the cases of IIDTRC. Jupe et al. (2016) suggests that effective vetting and the monitoring of staff are the first line of defence against employee's dishonest behaviours.

Law enforcement agencies such as the police have a vital role to play in IIDTRC prevention as they mainly have the necessary power and skills to take crimes cases beyond the reporting of incidents (Gottschalk & Hamerton, 2022). Besides, outsourcing for the specialist security agencies to deal with the IIDTRC incident assessments and reporting is recommendable. They can also play a major role on conducting internal data security vulnerability testing, and in educating employees on IIDTRC prevention measures. Efficient collaboration between law enforcement agencies and regulatory authorities is noted as one of the most effective preventive strategy against IIDTRC for any business organisation. Though, taking legal action against the fraudster might be expensive but a stringent deterrent for others (Klerman & Shortland, 2022).

Moreover, both the employees and stakeholders in the retail industry are expected to make more than just economic contributions. IIDTRC prevention responsibility should not be made to be the task of management alone. Researchers suggested that the concept of corporate digital responsibility (CDR) should be introduced in information security management as it has been applied in other management sectors (Jones & Comfort, 2022). Incorporation of CDR and other motivation factors promote good internal data security culture that would reduce incidents of IIDTRC in the retail industry.

3.2 RBF as a Model to Analyse Prevention of IIDTRC

The findings show that management of the organisations under study have relatively varying conceptions about their respective roles and responsibilities. Their conceptions about data security related issues are different from that of the outsourcing companies and front-line managements. The uneven clarity of crime prevention strategies, and paralleled sharing of roles pose challenge in implementing data security strategies. This finding confirms the hypothetical assumption of ORT that unclear roles and responsibilities among the management may create ambiguity 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 crimes awareness. The data compliance management have also designed auditing routines and used coercive strategy to ensure that the outsourcing firms are abiding to norms of data security policy.

This strategic learning approach by the top management agrees with recommendation of the RBF approach which explains the impact of clear roles and responsibilities across all the actors involved in prevention of these crimes. Haislip et al. (2021) found that CEOs with IT expertise and the presence of Chief Information Officers in top management level are significantly associated with fewer data breaches. Another notable finding is that the retail organisations under study have apparently no culture of crimes incidents analysis or strategy assessment. The management accepted that the prosecution of criminals closes the incidents case. They believe that reoccurring of crimes provides enough experiences needed to tackle potential incidents. This is contrary to the suggestions of RBF which emphasises the importance of IIDTRC incident report and assessment. RBF suggested that crime incident analysis and assessment reduce the risks of similar crimes in future. It would provide a clue for the crime prevention management. In agreement with the RBF, Majhi et al. (2021) noted that for an 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.

Yet counter to these suggestions, while employees' training and analysis of IIDTRC cases are more likely to lead to effective prevention of IIDTRC, this study findings indicate that these strategies are not implemented due to some constraints such as finance, employees' attitudes. This finding agrees with Chatterjee and Ray (2022) that financing staff training is one of the challenges of IIDTRC within any socio-economic setting even when there is a clearer strategic plan. On the other hand, this study shows that management is also faced the challenges of classifying the different types IIDTRC risks and incidents. These issues often lead to segregated data security strategy which has great impact in allocation of the available resources. This finding also agrees with Abdulsalam and Hedabou (2022) which noted that managements often struggle to prioritise security action plans; they always face the difficult decision of choosing either low cost action with high risks/impacts or long-term interventions.

4 Conclusion and Further Research

We have described some of the identifiable challenges of IIDTRC prevention. We have also used RBF as a model to analyse the management roles and practices that would enhance strategic prevention of IIDTRC in the retail industry. This research contributes to practice by identifying the

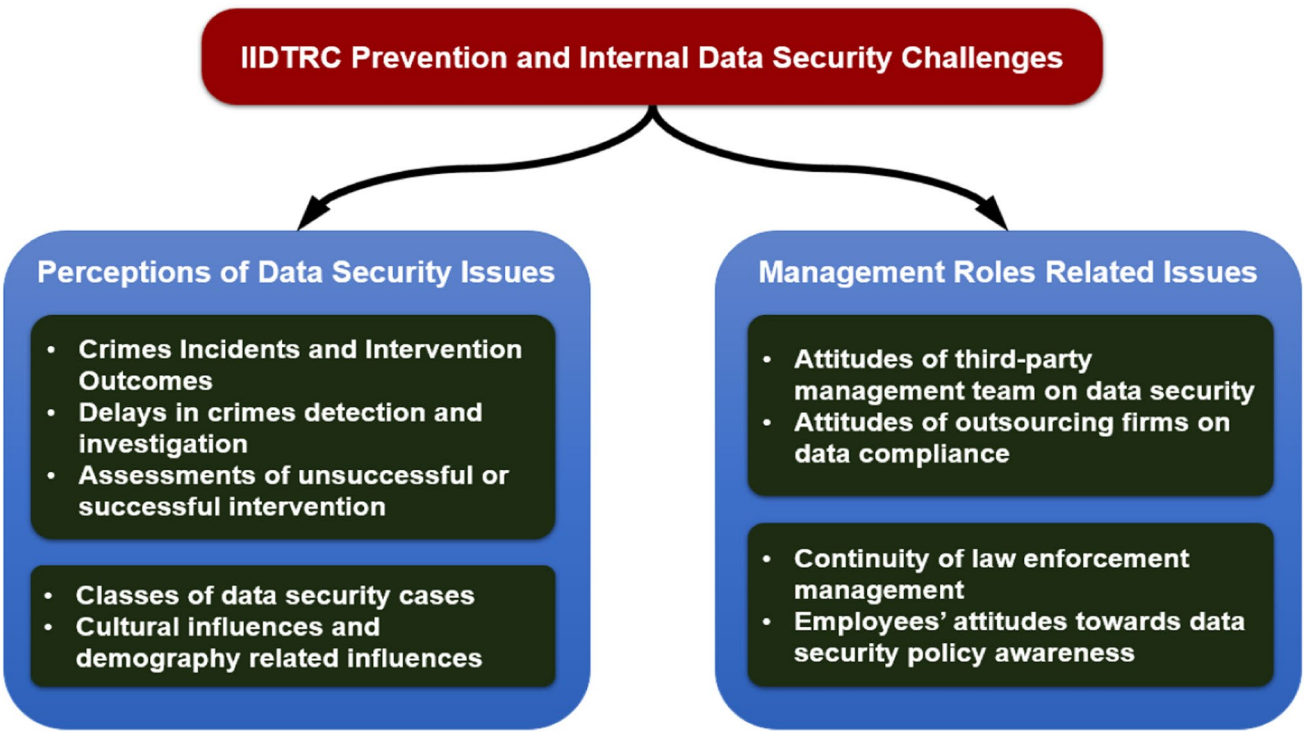

Fig. 4 Internal data security challenges of management on prevention of the IIDTRC

Table 3 Percent agreement and Cohen's Kappa Coefficient: coding reliability rating

File	File Folder	File Size	Kappa	Agreement (%)	A and B (%)	Not A and Not B (%)	Disagreement (%)	A and Not B (%)	B and Not A (%)
IIDTRC interviews with parent nodes	Files	13910 chars	0	68.57	0	68.57	31.43	0	31.43
IIDTRC interviews with parent nodes	Files	13910 chars	1	100	0	100	0	0	0
IIDTRC interviews with parent nodes	Files	13910 chars	0	92.14	0	92.14	7.86	0	7.86
IIDTRC interviews with parent nodes	Files	13910 chars	0	94.72	0	94.72	5.28	0	5.28
IIDTRC interviews with parent nodes	Files	13910 chars	0	95.31	0	95.31	4.69	0	4.69
IIDTRC interviews with parent nodes	Files	13910 chars	0	82.44	0	82.44	17.56	0	17.56
IIDTRC interviews with parent nodes	Files	13910 chars	0	65.56	0	65.56	34.44	0	34.44
IIDTRC interviews with parent nodes	Files	13910 chars	0	93.96	0	93.96	6.04	0	6.04
IIDTRC interviews with parent nodes	Files	13910 chars	0	94.57	0	94.57	5.43	0	5.43
IIDTRC interviews with parent nodes	Files	13910 chars	0	97.32	0	97.32	2.68	0	2.68
IIDTRC interviews with parent nodes	Files	13910 chars	0	91.04	0	91.04	8.96	0	8.96
IIDTRC interviews with parent nodes	Files	13910 chars	0	97.32	0	97.32	2.68	0	2.68
IIDTRC interviews with parent nodes	Files	13910 chars	1	100	0	100	0	0	0
IIDTRC interviews with parent nodes	Files	13910 chars	1	100	0	100	0	0	0
IIDTRC interviews with parent nodes	Files	13910 chars	1	100	0	100	0	0	0
IIDTRC interviews with parent nodes	Files	13910 chars	1	100	0	100	0	0	0
IIDTRC interviews with parent nodes	Files	13910 chars	1	100	0	100	0	0	0
IIDTRC interviews with parent nodes	Files	13910 chars	1	100	0	100	0	0	0

Table 3 (continued)

File	File Folder	File Size	Kappa	Agreement (%)	A and B (%)	Not A and Not B (%)	Disagreement (%)	A and Not B (%)	B and Not A (%)
IIDTRC interviews with parent nodes	Files	13910 chars	0	65.87	0	65.87	34.13	0	34.13
IIDTRC interviews with parent nodes	Files	13910 chars	0	91.73	0	91.73	8.27	0	8.27
IIDTRC interviews with parent nodes	Files	13910 chars	0	76.69	0	76.69	23.31	0	23.31
				Average = 90.82			Average 9.18		

internal data security challenges and prevention practices; and to theory by developing a role-based framework: an integrated role clarity approach that devolves the collaboration of shared roles to managements involved in the information security and crimes prevention in retail companies. As a corollary, this research suggests 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. Though, it is less practicable for the management team to implement the best data security roles and practices by only trainings and coercive 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.

However, this study is not without limitations. First, although the study was detailed case studies, it consists of only four retail firms in the UK. Future research can be extended to additional retail firms that span across the UK. Secondly, although the qualitative case study adopted in this research provides an in-depth description of IIDTRC, more substantial data can be collected through participant

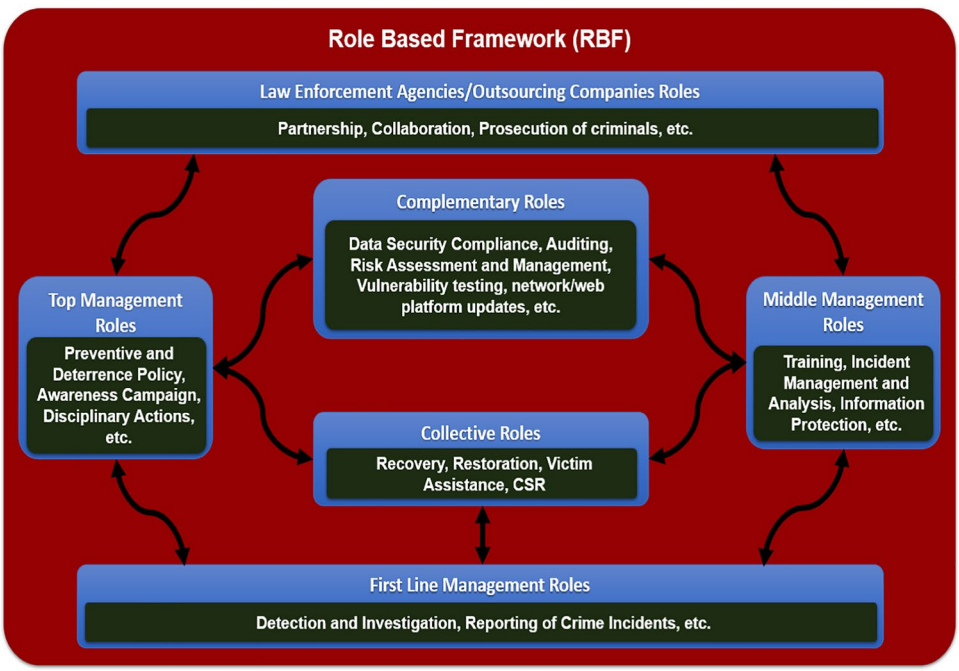

Fig. 5 Role based framework

observation or questionnaire survey to refine and test our findings. The following hypothesis that arises from this study can be tested:

1) *Retail management with clear data security roles tend to be more successful in using coercive strategies for prevention of IIDTRC; and*
2) *In retail industry where the internal data security management is poor, coercive strategies will lead to short term IIDTRC prevention; on the long term, management with clear roles might produce better results compared to coercive strategies. The results can be used to develop predictive tools or guidelines such as diagnostic systems to help practitioners in the field of information security.*

Future research can observe how managements carry out the data security roles and handle a typical IIDTRC incident in multicultural business context. In addition, further research can involve cross-case analysis using systematic research approach for validation of the RBF using participant observation and convergent interviews. It could be done by monitoring the processes and evaluating the internal data security resources. Researchers suggested that integrating resource priority and constraint plans in any crime prevention would enhance its generalisability. The potential findings will help to identify and prioritise the key concepts of the RBF model and develop plans to address resource constraints.

Declarations

Conflict of Interest The authors declare no competing interests.

References

Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. *Future Internet, 14*(1), 11.

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 20 April 2014.

Amasiatu, C. V., & Shah, M. H. (2018). First party fraud management: Framework for the retail industry. *International Journal of Retail & Distribution Management*.

Barling, J. (1995). International Review of Industry and Organisational Psychology. 11 (1). Wiley, UK.

Bernard, H. R. (1994). *Research Methods in Anthropology: Qualitative and Quantitative Approaches* (2nd ed.). Alta Mira Press.

Biddle, B. J. (1986). Recent developments in role theory. *Annual Review of Sociology, 12*, 67–92.

Biegelman, M. T. (2009). Identity Theft Handbook: Detection, Prevention and Security. (edn). Wiley.

Biglari, V., & Pourabedin, Z. (2022). Application of Data Analysis and Big Data in Auditing. In Community Empowerment, Sustainable Cities, and Transformative Economies (pp. 111–128). Springer, Singapore.

British Retail Consortium (BRC). (2015). 'BRC Retail Crime Survey 2014'. Available at: http://www.sbrcentre.co.uk/images/site_images/14591_BRC_Retail_Crime_Survey_2014.pdf. Accessed 10 January 2015.

British Retail Consortium (BRC). (2019). 'BRC 2019 Retail Crime Survey'. Avalable at: https://brc.org.uk/media/404253/brc-annual-crime-survey-2019.pdf.

Bryman, A. (2001). *Social Research Methods*. Oxford University Press.

Cabri, G., Ferrari, L., Leonardi, L., & Quitadamo, R. (2006). 'Collaboration-Driven Role Suggestion for Agents'. Proc. of IEEE Workshop on Distributed Intelligent Systems - Collective Intelligence and Its Applications, Prague, Czech.

Carley, K. M. (1993). Coding choices for textual analysis: A comparison of content analysis and map analysis. *Sociology Methodology, 23*, 75–126.

Centre for Retail Research. (2015). European Online Growth, Available at https://www.retailresearch.org/onlineretail.html

Chatterjee, U., & Ray, S. (2022). Security Issues on IoT Communication and Evolving Solutions. In Soft Computing in Interdisciplinary Sciences (pp. 183–204). Springer, Singapore.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model. Information Systems Research.

Chen, P., & Rohatgi, P. (2008). 'IT Security as Risk Management: A Research Perspective'. *IBM Research Report*. Thomas J. Watson Research Centre, Yorktown Heights, NY, USA.

CIFAS. (2021). Fraudscape, CIFAS, London, UK.

Collins, J. M. (2006). *Preventing Identity Theft in Your Business*. Wiley.

Cross, C., & Layt, R. (2021). "I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. Social Science Computer Review, p.0894439321999311.

Eisenhardt, K. M. (1989). Building theories from case study research. *Journal of Academic Management., 14*(4), 532–550.

Ekblom, P. (2010). *Crime Prevention, Security and Community Safety with the 5Is Framework*. Palgrave Macmillan.

Falotico, R., & Quatto, P. (2015). Fleiss' kappa statistic without paradoxes. *Quality & Quantity, 49*(2), 463–470.

Gottschalk, P., & Hamerton, C. (2022). Online Convenience. In White-Collar Crime Online (pp. 37–61). Palgrave Macmillan, Cham.

Guéraiche, W. (2022). Cyberspace, threat agents and power. Facets of Security in the United Arab Emirates, pp.76–86.

Haislip, J., Lim, J. H., & Pinsker, R. (2021). The Impact of Executives' IT Expertise on Reported Data Security Breaches. Information Systems Research.

Hakim, C. (2000). Research Design: Successful Designs for Social and Economic Research. 2nd (edn). London, Routledge.

Ho, S. M., & Warkentin, M. (2017). Leader's dilemma game: An experimental design for cyber insider threat research. *Information Systems Frontiers, 19*(2), 377–396.

Hodgson, G. M. (2006). What are Institutions? *Journal of Economic Issues, 40*(1), 1–20.
Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers, 15*(1), 1–4.
Johnston, A., Di Gangi, P., Howard, J., & Worrell, J. L. (2019). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems, 20*(3), 3.
Jones, P., & Comfort, D. (2022). Corporate Digital Responsibility: Approaches of the Leading IT Companies. Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies, pp.231–248.
Jupe, L., Vrij, A., Leal, S., Mann, S., & Nahari, G. (2016). The lies we live: Using the verifiability approach to detect lying about occupation. Journal of Articles in Support of the Null Hypothesis, 13(1).
Kahn, R. L., & Katz, D. (1978). *The social psychology of organizations* (2nd ed.). Wiley.
Katz, D., & Kahn, R. L. (1966). 'The social psychology of organizations. (edn). Wiley.
Klerman, D., & Shortland, A. (2022). The transformation of the art market: Law, norms, and institutions. *Theoretical Inquiries in Law*, *23*(1).
Kroll Global Fraud Report. (2010). Available at: http://ethicsline.com/pdf/kroll-global-fraudreport-english-usapr10.pdf. Accessed 23 September 2011.
Kroll Fraud Report. (2011). http://www.krollconsulting.com/insights-reports/global-fraud-reports/.
Lawrence, T., Suddaby, R., & Leca, B. (2009). Institutional Work: Refocusing Institutional Studies of Organisation. *Journal of Management Inquiry 20*(1), 52–58.
Luhmann N. (2004). *Law as a Social System* (pp. 64–66). Oxford, UK: Blackwell.
Luo, X. R., Li, H., Hu, Q., & Xu, H. (2020). Why individual employees commit malicious computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems, 21*(6), 5.
Lyytinen, K., & Grover, V. (2017). Management misinformation systems: A time to revisit? *Journal of the Association for Information Systems, 18*(3), 2.
MacQueen, K. M., McLellan, E., Kay, K., & Milstein, B. (1998). Codebook development for team-based qualitative analysis. *Cam Journal, 10*(2), 31–36.
Madsen, M. T. (2002). 'Managerial roles in a dynamic world', Proceedings of the 12th Nordic Conference on Small Business Research, Finland.
Majhi, S. G., Anand, A., Mukherjee, A., & Rana, N. P. (2021). The Optimal Configuration of IT-Enabled Dynamic Capabilities in a firm's Capabilities Portfolio: A Strategic Alignment Perspective. Information Systems Frontiers, pp.1–16.
McHugh, M. L. (2012). Interrater reliability: The kappa statistic. *Biochemia Medica, 22*(3), 276–282.
Mertens, D. M. (2003). Mixed methods and the politics of human research: Then transformative-nemancipatory perspective. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social & behavioral research* (pp. 135–164). Sage.
Mirza, N. A. S., Abbas, H., Khan, F. A., & Al Muhtadi, J. (2014). Anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms. *International Symposium on Biometrics and Security Technologies (ISBAST), 2014*, 126–132.
Okeke, R. I. (2015). The prevention of internal identity theft-related crimes: a case study research of the UK online retail companies (Doctoral dissertation, University of Central Lancashire).
Okeke, R., & Shah, M. (2016). *Information theft prevention: Theory and practice*. Routledge.
Organisation for Economic Cooperation and Developement (OECD), (2008). 'Policy Guidance on Online Identity Theft', OECD Ministerial Meeting on the future of the Internet Economy Seoul.
Pettigrew, A. M. (1990). Longitudinal field research on change: Theory and practice. *Journal of Organisational Science, 1*(3), 267–292.
Potter, C., & Waterfall, G. (2012). PriceWaterCooper's Information security breaches survey: Technical report [Available Onlince at www.infosec.co.uk].
Romanosky, S., & Telang, R., & Acquisti, A. (2008). Do Data Breach Disclosure Laws Reduce Identity Theft? Seventh Workshop on the Economics of Information Security, Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, NH, pp. 1–15
Salam, A. F., Dai, H., & Wang, L. (2021). Online Users' Identity Theft and Coping Strategies, Attribution and Sense of Urgency: A Non-Linear Quadratic Effect Assessment. *Information Systems Frontiers*, pp.1–20.
Sarnecki, J. (2005). Knowledge-based crime prevention, theoretical points of departure for practical crime prevention. In *Paper presented at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 18 – 25 April 2005, Bangkok, Thailand* (pp. 1–11).
Security, I. (2015). *Collaborative Security: An Approach to Tackling Internet Security Issues* (pp. 1–6). Creative Commons.
Shah, M. & Clarke, S. (Eds.) (2009). E-banking Management: Issues, Solutions and Strategies. London, UK: IGI Global.
Shah, M, & Okeke, R. (2011). Framework for Prevention of Identity Theft Related Crimes in UK Retail Industry. Proc. of Intelligence and Security Informatics Conference (EISIC).
Shopon, M., Hossain Bari, A. S. M., Bhatia, Y., Narayanaswamy, P. K., Tumpa, S. N., Sieu, B., & Gavrilova, M. (2022). Biometric System De-identification: Concepts, Applications, and Open Problems. In Handbook of Artificial Intelligence in Healthcare (pp. 393–422). Springer, Cham.
Stalla-Bourdillon, S. (2014). Privacy Versus Security… Are we done yet?. In Privacy vs. Security (pp. 1–90). Springer, London.
Stickley, J. (2009). *The Truth About Identity Theft. Why be me when I can be you?* USA: Pearson Education New Jersey.
Strauss, A., & Corbin, J. (1998). *Basics of qualitative research* (2nd ed.). Sage.
Wakunuma, K. J., & Stahl, B. C. (2014). Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues. *Information Systems Frontiers, 16*(3), 383–397.
Walsh, G., Shiu, E., Hassan, L., Hille, P., & Takahashi, I. (2019). Fear of online consumer identity theft: Cross-country application and short scale development. *Information Systems Frontiers, 21*(6), 1251–1264.
Weber, R. P. (1990). *Basic Content Analysis*. Sage Publications.
Wyre, M., Lacey, D., & Allan, K. (2020). The identity theft response system. *Trends and Issues in Crime and Criminal Justice, 592*, 1–18.
Xie, Q. (2013). Agree or disagree? A demonstration of an alternative statistic to Cohen's Kappa for measuring the extent and reliability of agreement between observers. In Proceedings of the Federal Committee on Statistical Methodology Research Conference (vol. 4).
Yin, R. K. (1984). *Case study research: Design and methods*. Sage.
Zhang, Y., & Yin, J. (2006). A Role-Based Modeling for Agent Teams. Proc. of 2006 IEEE Workshop on Distributed Intelligent Systems - Collective Intelligence and Its Applications, Prague, Czech.
Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management, 47*(2), 115–123.

Dr. Romanus Izuchukwu Okeke is a Senior Lecturer in Project and Operations Management (POM) in the School of Management, Cardiff Metropolitan University, Cardiff Wales, UK. Prior to this role, he was a Lecturer in POM at the Lancashire School of Business and Enterprise University of Central Lancashire (UCLan) where he received Ph.D. in POM (focused on Cybersecurity), MSc in Computing, PG Cert in Business and Management Research Methods. Rom has over 11 years' experience of successfully leading multidisciplinary high-quality research and complex projects for SMEs, corporate and government organisations across UK and West Africa, including 'Study of critical success factors of SMEs Productivity in the UK; project evaluation of UK Home Office funded £4.1 M UK Police Innovation Project at Lancashire Constabulary Headquarters, and Office for Students funded 4.3 M National Collaborative Outreach Programme at UCLan.

Rom is PRINCE2 certified and a passionate researcher with an outstanding track record in the areas of Identity Theft Prevention, Project Analytics, Data Science & Cybersecurity, Projects and Operations Risk Modelling, Operations Research & Decision Sciences. Rom is a member of the Association of Project Management, Institute of Operations Management and UK Society of Research Software Engineering. He has published in selected peer-reviewed academic journals and conferences as well as workshops including Routledge, Westminster Briefing, The Institute for Small Business and Entrepreneurship, and the British Academy of Management.

Dr. Max Hashem Eiza is a senior lecturer in computer security at the School of Computer Science and Mathematics, Liverpool John Moores University (LJMU). Max received his PhD in secure QoS routing in vehicular networks from Brunel University London in 2015. Max's research interests revolve around cybersecurity and data privacy issues in distributed and cyber-physical systems with the aim of developing novel schemes/protocols for various applications. During his career, Max published over 20 journal and conference papers.