2022-08-31

The realities of e-retailing in a pandemic world using data-driven training and awareness programmes to rethink e-retail fraud prevention strategies

Nwoko, Chiwuokem

http://hdl.handle.net/10026.1/20037

https://virtual.oxfordabstracts.com/#/event/1821/submission/384

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.
The realities of e-retailing in a pandemic world – using data-driven training and awareness programmes to rethink e-retail fraud prevention strategies.

Authors:

1. **Chiwuokem Nwoko**  
   PhD Researcher in Strategy and Applied Management at the Centre for Business in Society (CBiS), Coventry University (UK).  
   Contact address: Jaguar Building, Gosford St, Coventry CV1 5DL.  
   Email: nwokoc2@coventry.ac.uk

2. **Maureen Meadows**  
   Professor of Strategic Management at the Centre for Business in Society (CBiS), Coventry University (UK).  
   Contact address: Jaguar Building, Gosford St, Coventry CV1 5DL.  
   Email: ac3495@coventry.ac.uk

3. **Alexeis Garcia-Perez**  
   Professor of Management Information Systems at the Centre for Business in Society (CBiS), Coventry University (UK).  
   Contact address: Jaguar Building, Gosford St, Coventry CV1 5DL.  
   Email: ab1258@coventry.ac.uk

4. **Justin Okoli**  
   Senior Lecturer (PhD) - Department of Management & Entrepreneurship at the Leicester Castle Business School, De Montfort University (UK).  
   Contact address: The Gateway, Leicester, LE1 9BH.  
   Email: justin.okoli@dmu.ac.uk
Abstract

E-retail has steadily been on the rise because it is more convenient for most people. The COVID-19 pandemic has pushed people more into e-retail as they face lockdowns/choose to avoid social contact. This means that digital fraud is also rising, and retailers are scrambling to adapt to this new reality. Current literature reveals that fraud prevention training and agile fraud learning processes in e-retail firms are limited. However, there is limited research extended to data-driven fraud education from the perspective of the e-retail industry.

We evaluate the use of data-driven training and awareness programmes for e-retail fraud prevention. Data was collected through semi-structured interviews from expert participants in e-retail firms. Preliminary findings indicate that e-retailers should leverage data to improve their fraud training and awareness practices because limited latent data-driven fraud education programmes impede the development of e-retail fraud prevention.

Word count: 1,987 words (excluding cover page, tables, and references)

Keywords: Big Data, Digital Fraud, E-retail Fraud Prevention, Data-driven Fraud Training and Awareness, Data-driven Knowledge
Introduction

The key concepts that drive this study are digital fraud, e-retail and big data. Digital fraud refers to a type of fraud that aims to maliciously access and seize sensitive information by intercepting electronic exchanges like login credentials and emails (Cox, 2017). This can be done using malware\(^1\), weak company networks or unsecured public networks, eavesdropping techniques or even insider threats (Cox, 2017). In 2018, global card losses associated with digital fraud were projected to exceed US$1.3 billion (Accenture, 2018).

E-retail refers to electronic retailing where retail is conducted online and consumers engage with the retailer through a technical interface e.g., a website or mobile application (Kim & Lennon, 2012; Quill, 2018). Big data refers to large data sets that are voluminous and more complex to manage/process through traditional means (Xiaolong, et al., 2015).

E-retail has steadily been on the rise because it is more convenient for most people. The COVID-19 pandemic has pushed people more into e-retail as they face lockdowns/choose to avoid social contact (Morgan, 2020). The Office for National Statistics (ONS) reports that e-sales has grown by over 10% when comparing the period of the pandemic to pre-COVID levels and has remained over 50% higher than the start of 2020 (Dalgleish, 2020).

This means that digital fraud is also rising, and retailers are scrambling to adapt to this new reality (Vader et al., 2020). For example, in the UK, Action Fraud UK reports that more than £16 million have been lost to e-retail fraud during the COVID lockdown (Sims, 2020).

Providing training and educational/awareness programmes is an important aspect of the Human Resource Management of organisations (Nair & Maria, 2019). Since e-retail firms are reliant on digital resources (big data) for e-payments and e-commerce, they are susceptible to digital fraud. Therefore, e-retail management should consider the benefits data could deliver to comprehensive fraud education, skills, and training because the management bears the burden or consequences of any security risk or data breach that occurred, not the IT developers (Davenport, et al. 2012).

For example, Dixons Carphone retail group received the highest possible pre-GDPR (General Data Protection Regulation) fine of £500,000 from the Information Commissioner’s Office (ICO) after a 2018 data breach involving millions of payment cards details and other personal records that were compromised (Scroxton, 2020). However, the emergence of GDPR increases the scale of fines to four percent of global turnover or up to £17 million (GDPR, 2020).

Data-driven training and awareness have long been used in other data-driven industries e.g., in banking (Khanna & Arora, 2009) or hospitality (Wang, et al., 2018) with significant positive outcomes. However, there is limited research extended to data-driven fraud training and awareness from the perspective of the e-retail industry.

Examining the issue of data-driven fraud training and awareness from the perspective of the e-retail industry is essential because current literature reveals that there is limited fraud prevention training taking place (Khanna & Arora, 2009), and this is a significant issue particularly for e-retail firms (Shah et al., 2019). This inadequate training impedes agile fraud learning processes within the e-retail industry (Shah et al., 2019).

Wang, et al. (2018) argued that it is essential for firms that are collecting, storing, and processing data to develop big data capabilities and transform them into big data-driven

---

\(^1\) A malicious software designed to cause damage, collect data, or take control of a computer, computer network or server – e.g., computer worms, viruses, ransomware, spyware, trojan horse etc (Moir, 2009).
practices to derive benefit dimensions. Since the main organisational resource of e-retail firms is data, it becomes a necessary tool for them to derive strategic fraud prevention benefits through data-driven fraud training and awareness.

We aim to evaluate the use of data-driven training and awareness programmes for e-retail fraud prevention. This will bridge the gap in the existing literature in the following ways. (1) By extending the data-driven training and awareness discourse to the e-retail fraud prevention context. (2) By offering practical implications about data-driven fraud training and awareness and how e-retailers can reconsider their practices and assess whether their fraud prevention measures are tackling the concerns of digital fraud prevention. The following literature review reveals why data-driven training and awareness is key to answering this problem.

Literature Review

Existing research emphasizes the significance of knowledge in firms (Wiredu, 2012). Most firms focus on creating and supporting staff with a knowledge-oriented and agile learning environment (Henttonen et al., 2016; Annosi et al., 2018). Hence, firms consider knowledge as a leading resource (Wang et al., 2014), and employees must partake in learning processes to enhance knowledge (Sedighi et al., 2018).

Fraud management has risen to the top of the agenda of businesses in recent years (Camillo, 2016) and there are calls for practice-based fraud prevention studies that are replicable and relevant to managements (Huang et al., 2014; Peppard et al., 2014). Firms must have a robust structure of internal controls and employment procedures to avoid fraud (Khanna & Arora, 2009). Several studies (e.g., Aranda-Mena & Steward, 2005; Herold, 2006) have argued for the need for fraud training and awareness. Recently, a study by Shah et al., (2019) revealed that the strategy for learning processes in fraud prevention is weak in e-retail firms.

In today’s digital business climate, assisting employees learn how to spot and report fraud is particularly essential (Herold, 2006). A fraud training and awareness programme must be incorporated within the fraud prevention policies of a firm and be an integral part of the job evaluation process (Herold, 2006). A study found that a majority of fraudsters are in-house and their motivations to perpetrate fraud arose from “a lack of understanding” (Omar & Nawawi, 2016:1012).

E-retail firms must identify the limitations of learning processes (e.g., training and awareness) of fraud prevention and take necessary steps to ensure an efficient learning environment (Shah et al., 2019). Employees of e-retail firms deal with customers and company data, therefore their knowledge of fraud issues must be enhanced to protect data from fraud perpetrators (Yildirim, 2016).

By using big data tools, firms expect to derive benefits over several areas, like security (Chen et al., 2012). The gains organisations recognise as value is dependent on their strategic objectives for embracing and utilising big data (Ghoshal et al., 2014). Therefore, since the main challenge of e-retail firms concerns digital fraud and their main organisational resource is data, data becomes a necessary tool to derive strategic fraud prevention benefits through data-driven fraud training and awareness.
Methodology

We choose e-retailers as the case organisations for this study as they make up the e-retail sector. It poses an interesting critical case of organisations whose actions regarding data protection have frequently caused them to face increased legal and public scrutiny (ThreatMetrix, 2015; Kanya, 2018; Dickinson, 2019). This is likely to provide rich context because with the fast pace of technological advancement, consumer shopping patterns have changed and many ‘bricks and mortar’ retail stores and new entrants to the market have adopted e-retailing as an avenue of getting closer to consumers and enhancing sales (Yoo, et al., 2010).

We adopted a qualitative approach which is suitable when a researcher aims to ascertain deeper underlying meanings and explanations that cannot be obtained using quantitative methods (Rahman, 2017). For example, a survey cannot provide the underlying reasons why little fraud prevention training is offered in e-retail firms, thus, would present an insufficient analysis/probe. Data was collected through semi-structured interviews and the participants in the e-retail firms were selected according to their speciality of knowledge of data security, fraud prevention, and fraud education programme.

Semi-structured interviews were adopted because it allows for the collection of open-ended information on the use of big data for fraud training and awareness programmes from expert participants to explore their thoughts, beliefs and feelings about the subject and delve deeply into causal and correlated issues (DeJonckheere & Vaughn, 2019). Since our study is practice-based, we argue that practices (e.g., data-driven fraud training and awareness practices) should be observed and studied first with qualitative research methods (Huang, et al., 2014; Peppard, et al., 2014).

We interviewed 32 key/expert informants working substantially with data in 18 e-retail firms. These include data scientists, fraud analysts, strategists, operations and e-commerce managers, as well as a Chief Technology Officer, and Founder of a large e-retail firm. The sampling decision tree of our study is summarised in Figure 1.

Figure 1: The participant sampling decision tree
Our data analysis approached followed Bloomberg & Volpe’s, (2008) qualitative blended roadmap of deductive and inductive reasoning. Figure 2 summarises the roadmap of the data analysis of our study.

Figure 2: The roadmap for the qualitative data analysis process

Source: Adapted from Bloomberg & Volpe, (2008).
Preliminary Results

Our preliminary findings show that the overwhelming majority of the respondents indicated that there is a complete absence of (i.e., non-utilisation) or limited utilisation of data-driven fraud prevention training and awareness programmes across the e-retail sector.

A substantial number of respondents (10 participants, equivalent to 31% of the whole sample) reported that their e-retail firm does not use big data-driven insights to design fraud training and awareness programmes. This can be illustrated with the following statements in Table 1.

<table>
<thead>
<tr>
<th>Respondent:</th>
<th>Job role</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Chief Risk &amp; Data Officer</td>
<td>“No, our security training has nothing to do with big data.”</td>
</tr>
<tr>
<td>10</td>
<td>Fraud Intelligence Manager</td>
<td>“We are still in a discovery phase and infancy when it comes to the outside of the data team. We have not fully understood or explored the data we have especially for fraud prevention, but we are willing to.”</td>
</tr>
</tbody>
</table>

A majority of respondents (18 participants, equivalent to 56% of the whole sample) suggest that there is limited use of data-driven training and awareness programmes in e-retail fraud prevention. This can be illustrated with the following statements in Table 2.

<table>
<thead>
<tr>
<th>Respondent:</th>
<th>Job role</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>Business Data Analyst</td>
<td>“The bigger the data you have, the more the knowledge employees need to be aware of, so, this is important”</td>
</tr>
<tr>
<td>25</td>
<td>Cybercrime Policy Analyst</td>
<td>“The way we used to collect data has now changed with the coming of big data. Staff need to be trained on how to utilise that new information and how to leverage them for the benefit of organisations.”</td>
</tr>
</tbody>
</table>

These respondents indicated data-driven insights are not used for fraud prevention training and awareness programmes, and even when used, the priority of fraud training is role-based (priority on IT employees or technical staff), staff-level based (priority on senior management, i.e., top, and middle levels) and/or issue-based (priority tailored to address current business issues). This can be illustrated with the following statements in Table 3.

<table>
<thead>
<tr>
<th>Respondent:</th>
<th>Job role</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operations Manager</td>
<td>“Training is role-based. IT personnel are prioritized because they are the first point of contact with the data and require specialised skillset.”</td>
</tr>
</tbody>
</table>
More of the training goes to the middle and upper level because the lower levels have a lot of restrictions to what they can have access to. We give them comprehensive training because they are the ones exposed to the company’s data.”

Prioritisation of fraud training and education should be issue-based. Organisations should focus on what the current issue is based on interactions with employees and visual feedback from other departments in the organisation. Then customise training to directly address those issues by training and creating awareness of the policies or framework governing those issues and the consequences of not applying or obeying the policies.”

Only a small number of respondents (three participants, equivalent to 9% of the whole sample) reported that their e-retail firm fully implements organisation-wide data-driven fraud training and educational/awareness programmes regardless of staff level, role, or issues at hand. This can be illustrated with the following statements in Table 4.

<table>
<thead>
<tr>
<th>Respondent:</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 Client Service Associate</td>
<td>“We train our staff based on the requirements and insights we get from our data. Training cuts across all staff levels from the top to the bottom.”</td>
</tr>
</tbody>
</table>

Discussion and Way Forward

Our preliminary findings indicate the following. (1) Data-driven fraud educational programmes are not widely utilised in e-retail. (2) E-retailers should leverage data to improve their fraud training and awareness practices. (3) Limited latent data-driven knowledge, training and awareness capabilities and firm-specific routines impede the development of data-driven e-retail fraud prevention capabilities. (4) E-retail and traditional retail are not the same. The learning process required for fraud prevention capability formulation in the former varies from learning for building in-depth data-driven fraud prevention capability in the latter; the impartial distribution of data-driven fraud learning/training across e-retail firms is necessary for a better fraud prevention strategy.

Future work will analyse the critical factors affecting data-driven fraud training and awareness in e-retail from the perspective of expert informants/employees. It will aim to examine the theoretical and practical implications of data-driven fraud training and awareness programmes in e-retail firms especially in a pandemic-stricken world and after. Lastly, it will suggest ways forward for better data-driven fraud education inclusion in e-retail.
References


