Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT)

Completed Research Paper

Faisal Alanezi
Brunel University, UK
Faisal.Alanezi@brunel.ac.uk

Laurence Brooks
Brunel University, UK
Laurence.Brooks@brunel.ac.uk

Abstract

Online fraud, described as dubious business transactions and deceit carried out electronically, has reached an alarming rate worldwide and has become a major challenge to organizations and governments. In the Gulf region, particularly Saudi Arabia, where there is high Internet penetration and many online financial transactions, the need to put effective measures to deter, prevent and detect online fraud, has become imperative. This paper examines how online fraud control measures in financial institutions in Saudi Arabia are organized and managed. Through qualitative interviews with experts in Saudi Arabia, the study found that people's perceptions (from their moral, social, cultural and religious backgrounds) have significant effect on awareness and fraud prevention and detection. It also argues that technological measures alone may not be adequate. Deterrence, prevention, detection and remedy activities, together making General Deterrence Theory (GDT) as an approach for systematically and effectively combatting online fraud in Saudi.

Keywords

Online fraud, general deterrence theory, Saudi Arabia.

Introduction

Fraud has taken a new dimension as fraudsters invade the virtual/online world using various means and techniques to 'gain' money while exploiting the lack of attention and carelessness of individuals, organizations and general society (Deloitte, 2011). Modern online fraudsters are constantly inventing techniques, targeting virtual attacks on virtual wallets and online accounts of citizens (Brytting, Minogue & Morino, 2011). While there has been an increase in the use of facilities for online transactions, such as e-commerce and e-banking, there has also been remarkable carelessness in handling 'foreign' online funds and an increase in the use of online facilities for dubious business transactions (Hawkins, Yen and Chou, 2000; Albert, 2002). Combatting the threat of online fraud has therefore become a concern and a challenge to individuals, organizations and governments. Different countermeasures are known to have been adopted but the menace of online fraud continues.

Online fraud

Online fraud is generally described as the use of online facilities to carry out dubious business transactions with the intention of deceiving or defrauding persons, organizations or governments (Albert, 2002). The several dimensions of online fraud has brought complexity to the phenomenon which is mostly directed at causing huge financial losses to individuals, organizations and particularly financial institutions (Samociuk, Iyer & Doody, 2010). Online fraud is generally committed indirectly and most times "face-less" through computer software programs and other banking procedures, devices/machines.

Online fraud is qualified as a cybercrime defined legally as "a false representation by means of a statement or conduct made knowingly or recklessly in order to gain material advantage" (Martin, 2003: 211). The major element of the definition is gaining material advantage as a result of false representation; therefore false representation is regarded as a key component of online fraud. It is perpetrated in different disguise, forms or shades. Common forms include online identity theft and fraud, online retail schemes and online auction fraud.

Varieties of online fraud

A more structured approach to the varieties of online fraud was presented by the Internet Crime Complaint Center (ICCC Report, 2010), using the following classifications:

- Miscellaneous fraud: "variety of scams meant to defraud the public, such as work-at-home scams, fraudulent sweepstakes and contests, and other fraudulent schemes" (p. 18).
- Advance fee fraud: "criminals convince victims to pay a fee to receive something of value, but do not deliver anything of value to the victim" (p. 18).
- Auction fraud: a major crime scene occurs during auction or on an auction site (p. 18).
- Credit card fraud: where fraudsters use credit cards of another person in order to withdraw money illegally (p. 18).
- Overpayment fraud: where an "incident in which the complainant receives an invalid monetary instrument with instructions to deposit it in a bank account and to send excess funds or a percentage of the deposited money back to the sender" (p. 18).

The nature of online fraud therefore requires countermeasures using computer software, regulations and banking systems controls and devices to deter, detect and prevent it (Wells, 2010). Online fraud has also attracted a lot of attention from organizations and has prompted the need to minimize the damage caused by online fraud (Moore, 2010). One major reason most organizations have experienced the devastating effect of online fraud is the focus on profit rather than security (Best Company, 2010). This lack of focus and misplaced priorities, coupled with other factors such as traditionalism, conservatism and lack of adequate regulations have had negative impact on the countermeasures adopted by organizations in the gulf region (Arab Region Internet and Telecom, 2001).

The alarming rate of online fraud worldwide, even as governments and organizations have taken steps to combat it, has made the issue of its control and prevention a major challenge worldwide (Coyne, 2005; Montague, 2011). The argument therefore could be that the measures taken were either not sufficiently comprehensive, inadequate or have systematically failed to effectively address the issues of online fraud. This paper aims to examine how the deterrence, prevention and detection countermeasures of online fraud activities in organizations in Saudi Arabia have affected the rate of online fraud. The study will use the general deterrence theory (GDT) as a theoretical lens to conduct the investigation using a qualitative interpretive case study approach and a thematic data analysis.

Online Fraud in Saudi Arabia (SA)

Saudi Arabia (SA) is reported to be one of the wealthiest countries in the Middle Eastern region. It has the highest level of Internet penetration supported by government policies and the use of advanced technologies in most areas of governance and commerce. It has the highest number of Internet users, a 62.97% penetration level (Karake Shalhoub & Al Qasimi 2003), with the highest relative Cybercrime and fraud levels in the GCC region (Dwyer, 2010).

Online fraud is therefore a concern to the SA government not only because of the low awareness but also because of specific economic and social factors. A survey of the types of online fraud in SA shows a range of factors (see Table 1, Alfuraih, 2008).

№	Reason	VISA	MasterCard	Total
1	Merchant has no authorization	18.4	30.7	49.1
2	Authorization cancelled	2.69	4.61	7.3
3	Charged my expired card	1.15	2.11	3.26
4	Transaction not recognized	3.65	6.15	9.8
5	Cancelled recurring	0.57	0.57	1.15
6	Paid by other mean	8.84	0	8.84
7	Charged twice	4.8	3.65	8.45

№	Reason	VISA	MasterCard	Total
8	Service not rendered	4.8	1.53	6.33
9	Goods returned but not money	0.96	1.15	2.11
10	Item received late	2.69	0	2.69
11	Amount not correct	0.57	0	0.57
12	Incorrect currency	0.19	0	0.19

Table 1. Types of/Reasons for online fraud in SA

Other studies on online security have also indicated trust and lack of education as issues affecting online rate, problematic areas of online security have also been identified as: (1) user authorization; (2) entry points; (3) dynamic nature; (4) protection against manipulation; and (5) confidentiality (Ahmed, Buragga & Ramani, 2011; Alfuraih, 2008).

SA Banking Sector

The banking sector in SA has maintained asset growth above that of the GCC banking sector and credit growth in 2011 was regarded as the largest banking market in the GCC (Gulfbusiness, 2012). It has been noted that an increased public spending by the Kingdom transfers down the line through corporate loan demand and retail credit growth, which has had significant impact on the health of the Kingdom's banking sector. Strong government regulation and hefty public spending have therefore buoyed the Kingdom's banking sector (Buller, 2012).

Issues with Online Payment and Local Banking Systems

Online payments issues have received a higher focus and attention in e-commerce activities in SA. The issues raised are mostly concerned with the difficulty of getting credit/debit cards, fear of the card misuse which could result to money being stolen, credit cards fees which are linked with religious issues, and problems of international acceptance of some cards. These issues have presented some difficulties for most participants in e-commerce which have prevented many from buying online. The fear of losing card details or details being stolen by traders has also being a major concern for people in SA.

Theoretical Approach (GDT)

The General Deterrence Theory (GDT) has been chosen as the framework for the investigation and analysis of online fraud in SA. The components of GDT provide a theoretical framework to investigate the deterrence, detection, prevention, and remedy of online fraud. It enables an examination of the countermeasures and the effects on online fraud. Computer security theories such as (i) criminological theory; (ii) information systems security effectiveness theory; and (iii) situational crime prevention theory, focus on security environment and physical security, but GDT goes deeper by focusing on countermeasure activities and relationships and their collective effect on online fraud. GDT's four components include deterrence, prevention, detection, and remedy (Figure 1), based on the argument that individuals who commit crimes can be dissuaded from committing such crimes through the use of countermeasures (Straub & Welke 1998).

GDT views deterrence as influencing decision making which may require altering or reinforcing how the decision makers perceive key factors that need to be considered before they act (D'Arcy, Hovav, & Galletta, 2009). Deterrence is defined as the inhibition of criminal behavior through fear of punishment which is passive, relying on the individual for compliance. The aim of deterrence is thus to provide disincentives for potential computer fraudsters (Whitman 2004). GDT also posits that deterrence activities create awareness and inhibit fraud which could stop crimes before they are carried out (Chen, Ramamurthy & Wen, 2012; Jing & Pengzhu, 2011). Deterrence activities also help facilitate prevention activities by establishing necessary awareness for the operators of the system.

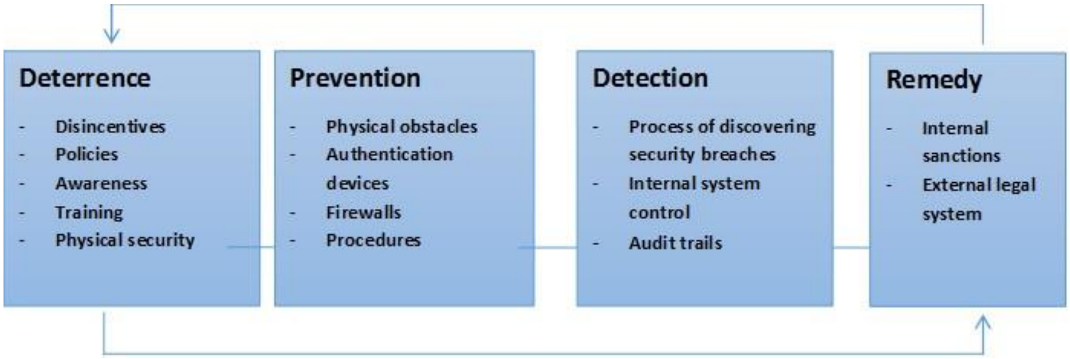

Figure 1. Elements of the General Deterrence Theory (GDT)

Methodological Approach

Qualitative research, designed to help understand people the social and cultural contexts within which they live, is used in this study (Myers 2009). It is an approach that allows the experiences of the people in the research focus to be examined in detail and from their perspectives, making it easier to achieve an understanding of the meanings and interpretations given to such issues. The natural settings of participants are used in the process of obtaining qualitative data in the form of words (text) through interviews and observation. Moreover, qualitative research is a means for exploring and understanding the meanings individuals or groups give to social and human problems (Creswell 2007).The qualitative research view of the social world highlights relationships and actions forming social life and the source of information about the creation of social life (Bryman 2001; Creswell 2007; Myers 2009). Thus it sets researchers closer to reality.

Qualitative data collection

Twenty-seven interviews were carried out with staff from four banks in SA. The participants were selected based on their functions in the banks and roles in the prevention of online fraud in their respective banks (Table 2). However, the general nature of the type of questions were about the existing countermeasures of online fraud in Saudi, such as regulation, people's perception about online fraud, their awareness levels and technological applications for combating online fraud.

Participants	Position/Function	Number interviewed
IT Bank staff	Risk managers IT technicians	10 3
Customer services	Services Managers Account Officers	4 4
Bank Customers	Account owners	3
Government regulators	E-commerce supervision	3

Table 2. Participants and their Positions

Analysis

The collection of textual data through the semi-structured interview requires a scientific and an artful qualitative analysis approach (Patton 1990; Corbin and Strauss 2008). Attride-Stiling (2001) suggests that using established methodological procedures and well accepted techniques, qualitative analysis can provide a rigorous and scientific approach to derive useful interpretation of the data collected. This confirms the interpretive nature of qualitative data analysis which will be useful for this research (Hennink et al., 2011).

There are different approaches to qualitative data analysis such as discourse analysis, narrative analysis, content analysis, thematic analysis and grounded theory. They all adopt similar procedures but different emphases and are useful in different situations and purposes (Hennink et al. 2011). The thematic analytical method is the chosen method of qualitative analysis for this study. Its flexibility and independence from theories and epistemology, and its ability to both reflect reality and to pick or unravel the surface of reality makes it a useful method for this research (Braun and Clarke, 2006). Thematic analysis allows the researcher to identify and group patterns referred to as themes, in describing a dataset. It creates the opportunity for the researcher to reflect on the reality of the situation and unravel any hidden truth in the perception of the participants (Braun and Clarke, 2006).

Data Transcription

27 recorded interviews of one hour duration each were transcribed with the aim of retaining sufficient details of the interview and to give a near verbatim account of the interviews. The transcription process therefore involved a replay of the recorded interviews, coupled with a confirmation of the interview notes and matching any observed actions or happenings during the interview session. The rational is to recreate the interview, for a proper and better understanding of the dataset. This created a familiarity with the data, enhanced understanding of the issues and kick-started the initial development of ideas and meanings of the data (Riessman 1993; Lapadat & Lindsay 1999).

Coding

With the understanding gained and the generation of initial ideas, statements and comments were given initial codes based on their features and meanings. The process ensured that all statements were given initial codes in order to cover the entire data set. At the end of this initial coding, the features identified to be of interest to the research focus directly or remotely, were grouped into meaningful groups of segments and patterns that are related to the theoretical framework and coded accordingly. This second set of codes were checked and rechecked for duplication, omission and appropriateness. This resulted in the merging, expanding or scrapping and addition of some codes which finally produced the third set of codes. The final set of codes was checked for relationships and then sorted accordingly as sub themes. As a result four major themes with their sub-themes were identified (Table 3).

Themes	**Sub-Themes**	**Codes**
Perception	Points of view online fraud	Technology based/inspired/driven Game Deception
	Perception of online fraud	Criminal activity Antisocial Greed/hunger/not criminal
Awareness	Level of awareness	Lack of knowledge Training Lack of government sensitization Religious inclinations
	Frequency of occurrence	Personal experiences E-commerce activities Reporting status
Technological measures	Technological controls	Computer controls Procedural controls and checks Complex/Cumbersome operations Ignorance/Vigilance
	Control focus	Abuse/Unlawful use of computing resources Protecting confidential information of customers Illegal online activities
	Relevance and adequacy of measures	Safe and trustworthy Involvement of the customers Regular updates needed

Themes	Sub-Themes	Codes
Regulations	Types of regulations	Government regulations/laws In-house rules and guidelines
	Focus of the regulations	Internet monitoring Operational guidelines
	Impact of the regulations	Lack of awareness Lack of focus and purpose Need for internal rules

Table 3. Summary of themes and sub-themes.

Findings and Analysis

The detailed findings highlight key issues that have affected the growth of online fraud in SA, each of the four themes and sub-themes will be discussed in turn below.

Perception Theme (see Table 3)

This theme identified the meaning of online fraud and how the people see or perceive online fraud based on their cultural and societal beliefs and educational background. The sub theme online fraud definition has three codes that capture the meaning of online fraud as given by the participants. The codes are technology based/inspired/driven definition; game based definition; and deception based definition. The second sub theme looks at the perception of the people and how they regard online fraud. It has three codes capturing the way the participants see online fraud as a criminal activity, anti-social, and greedy and hunger driven activity and not a criminal activity.

Points of view of online fraud

The interpretation of the participants as regards the meaning and definition of online fraud shows three main definitions and classifications. Participants generally agree that online fraud is technologically driven and inspired, it is a game played by two or more players to outwit one another, and it is a life of deception based on lies and tricks using technological skills.

Technologically driven and inspired: As a computer engineered activity, participants believe that online fraud would not have been possible without the advent and use of the computers in business transactions and banking activities. The increase of online fraud is therefore attributed to the increased application of computers and its devices which has become the foundation and the driving force of online fraud in the country.

Online fraud as Deception: Another main description of online fraud is its deceptive nature exploiting the greed and foolishness of the people involved. It is claimed by most participants that only the greedy individuals and those who foolishly or ignorantly take everything at face value fall prey to deceptive tactics of online fraudsters.

Perception of the people on online fraud

Participants see implications of online fraud activities in different perspectives. This sub-theme captures the different perspectives and the way the participants see the activities of online fraudsters in the country. The three perspectives show that online fraud is a criminal activity; it is anti-social and against cultural beliefs; and greed and hunger induced therefore not criminal.

Criminal activity: The perception of most participants is that online fraud is a criminal activity with criminal intention to unlawfully take possession of another's property through crooked means. Two issues mainly highlighted in the categorization of online fraud as a criminal activity are the intention or mission of the act and the means or method used. Some participants however agree that a person that stole with the intention of satisfying his/her hunger should not be seen as a criminal.

Anti-social: Most participants also agree that online fraud is both socially and culturally out of order and does not represent the socio-cultural and religious beliefs of the nation. The perception is that because the culture and social norms of the land condemn stealing of any kind, online fraud is seen as a social taboo and a social crime.

Unfair gain induced non-criminal activity: The intention or the motive of the activity may determine how it is classified. Some participants therefore do not see fraudulent practices based on hunger as criminal but rather as a social problem that needs to be addressed socially. Other participants also attributed the occurrence of online fraud to the greedy get rich quick attitude of the victims. It is agreed that it 'takes two to tango' and that the welcoming posture of the greedy victims make room for the perpetration of online fraud.

Awareness Theme (see Table 3)

This theme acknowledges the importance of awareness, the issues surrounding the levels of awareness and the challenges these issues pose on online occurrences in the country. The data set highlights seven codes which capture the issues and challenges confronting awareness and online fraud. These codes are grouped into two sub-themes.

Level of Awareness

The level of awareness of online fraud is low in SA. This could be attributable to four issues identified as, lack of knowledge; training; lack of government sensitization and religious inclinations.

Lack of knowledge: Low level or complete lack of knowledge of online fraud which may be due to level of education and exposure to computers, and may have contributed to the low level of awareness of online fraud activities. The findings also show that the fraudsters took advantage of the victims' ignorance and their dependence on guidance. The findings show instances where computer illiterates unsuspectingly gave out their bank cards and details to relatives or friends to help carry out some financial transactions and were defrauded with the use of such account details by some faceless customers purporting to be the original account holders. Participants also agree that their perception of online fraud influence their knowledge and consequently their awareness.

Training: Training and education have been used to create some awareness of online fraud. The effect of this has also been positive on the fight against online fraud in the country. Some organizations and even private individuals have used training to expose the tricks and games of online fraudsters. Training and education are done in-house for both staff and customers using company social media and customer service advice given over the counter usually during account opening transactions or with e-commerce transactions.

Lack of government sensitization: The findings show that the lack of government sensitization contributed to the low level of awareness and the consequent rise of online fraud in SA. The government's relative silence about the activities of online fraudsters more or less created an impression that online fraud is not a crime. However as the cases of online fraud has increased in SA, the government focus has shifted from just monitoring Internet usage to publicity campaigns about online fraud.

Frequency of exposure of online fraud

This sub-theme captures the issues regarding the occurrence of online fraud and the challenges faced by the institutions and the victims. The findings identified three main issues affecting the frequency of occurrence and subsequently, online fraud in the country.

Personal experiences: The findings show that most people with personal experiences are those in businesses and those involved in e-transactions. It shows that the business community is becoming more aware of online fraud as they engage in e-commerce activities and fall victim to the practices of online fraudsters. The majority of online fraud cases reported are also business cases signifying the prevalence of business related fraud as the major type of online fraud. Most of the frauds are reported to have targeted unauthorized access to business accounts using false identities. Most participants agree that this may have caused an increased awareness to these types of online fraud.

E-commerce activities: Participants agree that there is an increase in electronic transactions as the government encourages adoption of ICT in different aspects of governance and economy. The involvement of more people in electronic business has thus opened up the challenges and problems usually associated with ICT adoption. This has therefore increased the awareness of online fraud and other dangers of using e-commerce. Participants also agree that the introduction of electronic banking to facilitate easy and comfortable banking services to the customers also opened avenues for fraudulent practices.

Reporting status: One major issue that may have affected the awareness of online fraud is the reporting of online fraud cases by the victims to the regulating authorities. The findings show that victims are reluctant to report incidences of fraud against them for many reasons. The failure or refusal to report online fraud has kept a lot of likely victims in the dark and does not create the necessary awareness. The failure of victims reporting cases is also attributed to be partly due to lack of proper confidential reporting procedures/systems. Major Banks have therefore been making attempts to introduce reporting structures to encourage victims to use available platforms to report and fight online fraud.

Technological Measures Theme (see Table 3)

This theme covers the investigation on the technological measures in place to check and control online fraud in the country. It captures issues that relate to the types of technological and procedural controls, how these controls are designed, their main targets or focus and the relevance or adequacy of the controls.

Technology controls

The findings show that most banks and other organizations, including the government, have realized the enormity of online fraud and have taken steps to stop the increasing wave of online fraud. While some organizations relied on technological controls, others emphasized the use of procedural and process controls and others a mixture of technology and procedural controls. Nevertheless the installation of these measures somehow makes most operations complex and cumbersome and may also require the vigilance and understanding of the operators and customers.

Computer controls: One basic measure taken is the installation of technological gadgets relied upon by most organizations because of the technological driven nature of online fraud. Participants also agree that there are different technologies designed to prevent and detect online fraud and other related computer crimes and fraudulent practices which are now put in place in some organizations. The majority of participants also believe that organizations have an obligation to protect their customers' assets and trust and are therefore responsible for installing appropriate measures to meet these demands.

Procedural controls and checks: The findings also indicate that most organizations rely strongly on procedural controls and checks to prevent and detect online fraud. These organizations suggest that most online fraud are as a result of loopholes in the procedures which fraudsters take advantage of regularly, and also due to lack of proper checks. Some organizations have also combined the procedural checks with the use of computer software and gadgets for a more effective fight against online fraud.

Complex/Cumbersome operations: The installation of technological measures and procedural controls however presented an issue highlighted by some participants. These measures elongated the process, made it complex while some customers found it cumbersome to follow through. The security questions, secret codes and passwords that have to be filled have been worrisome to most customers who often are not able to remember the needed answers to complete the transactions. The findings display that this issue has been a setback for most customers particularly the less educated and computer illiterates.

Ignorance/Vigilance: Another major issue highlighted is that in spite of the technological controls and procedural checks, online fraud has not been brought under control due to the ignorance of most customers and online users. Most customers ignorantly aid and facilitate online fraud which easily goes through the controls and checks. The findings also show that apart from the ignorance of the customers, the carelessness of some staff have also been exploited by the fraudsters.

Relevance and adequacy of measures

Participants also highlighted issues of relevance and adequacy of the technological measures in place. The issues raised include how safe and trustworthy the measures are, the role of the customers in the operation of the measures and making them effective, and necessary regular updates needed to sustain the effectiveness of the measures.

Safe and trustworthy: Most participants agree that considering the situation in SA, the present measures taken in combination of technological controls and procedural checks, are safe enough for whatever focus or concerns organizations may have. Some pointed out that the safety and adequacy of the measures have bolstered the confidence of the customers and enhanced their trust in the ability of the banks to protect their interests. However some participants are of the opinion that the measures are not foolproof but require constant monitoring and improvement.

Involvement of the customers: Participants also agree that the relevance and adequacy of the measures in place cannot be complete without the active positive participation of the staff and most especially the customers of the banks. The involvement of the customers is seen as vital to the effectiveness of the measures.

Regulations Theme (see Table 3)

This theme presents issues and challenges relating to regulations in SA and their impact on the prevention and combatting of online fraud. Three main issues and sub-themes that highlight the effectiveness of the regulations are types of regulations; focus of the regulations; and impact of the regulations.

Types of regulations

Most participants agree that the lack of appropriate and specific rules and regulations guiding online transactions in business may be the major loophole facilitating online fraud in SA. There are government rules and regulations guiding Internet operations which may be silent on rights and privileges of the customers. Banks and other institutions have also formulated rules and regulations to guide their activities.

Government regulations/laws: Main concerns raised relate to the inability of the government to establish a platform built on appropriate rules and regulations that acknowledges and stipulates rights and privileges of the consumers and defines what an abuse of rights is. Most participants depend on the government to set the stage for online transactions with clearly defined roles and responsibilities, but this is lacking.

In-house rules and guidelines: Acknowledging the importance of rules and regulations in online operations and with the lack of guiding principles from the government and its agencies, most organizations had to define the rules of play for their customers and staff as well.

Focus of the regulations

Most of the participants agree that the regulations are meant to provide a level playing field for all participants involved in online transactions, guiding their activities and protecting their rights. The picture however shows a different focus for the government rules.

Internet monitoring: The concern raised is that the government's regulations are focused on monitoring Internet usage and therefore have not done much in deterring, preventing and detecting fraud. However, the rules and regulations formulated by private organizations such as the banks are more focused on deterring, preventing and detecting fraud with little success.

Operational guidelines: Another major focus of both government regulations and in-house regulations is the provision of operating guidelines for individual users and organizations.

Discussion

It is noted that the findings have helped in putting a structure to enhance the prevention and detection of online fraud and there is a clear indication that the mindset of the people which was based on their moral, social, cultural and religious inclinations and background, formed their different opinions and perceptions of online fraud. While some of the people see online fraud as a criminal activity and a social crime, others do not see it as a crime but a game played by insatiable people. This mixed opinion and perception of online fraud has also affected the level of awareness and occurrence of online fraud.

As a result of these perceptions, the level of awareness of online fraud in SA is low. This also has a significant consequence on fraud prevention and detection. Organizations where awareness campaigns were carried out showed low rates of online fraud, implying effective prevention and detection due to the alertness of the people. Both staff and customers where better trained which helped to deter and prevent fraud. The increase in the number of occurrences was also seen to increase awareness as it gave the people hands-on experience.

However, the increase in online fraud occurrences also implies effective detection and possibly a failure in the preventive arrangements to stop the fraudulent intentions/activities before they were detected. This suggests that although organizations have put into place relevant technological measures coupled with procedural controls and checks, these measures alone may not be adequate to prevent and detect online fraud.

Implications of findings

The study suggests that deterrence, prevention, detection and remedy activities need to work together for any effective combatting of online fraud (Kotulic & Clark 2004). Better coordination of relationships and interactions between these components are critical success issues. The success of any effort or approach to combat online fraudulent activities depends on the activities of these four components which must be visibly seen to be in operation in the organization (Whitman 2004).

Contribution

The framework resulting from the study (see Figure 2, below) shows that the social cultural environment, industrial environment and organizational environment have significant influence on countermeasure activities of deterrence, prevention, detection and remedy of online fraud. The influence of these environments on the people, organization, practices, and also on the measures used to combat online fraud can be used as channels to positively provide counter measures to online fraud. Deterrence activities create awareness and inhibit fraud which could stop crimes before they are carried out. Combating online fraud in Saudi Arabia should not rely solely on technological measures. The social environment could be tailored to guide a positive perception of online fraud and create necessary awareness of the problems of online fraud and the consequences. This could serve as an effective deterrence.

Limitations

This research is based on a relatively limited number of interviews with people informed about banking in SA. Future research might expand this set to a wider group of experts in SA and further into the wider GCC. However, this paper shows that a useful starting point for raising awareness of these issues is important, to begin to discuss online fraud more openly and find better ways to protect both individuals and organizations.

Practical implications

A systematic approach to the organization and coordination of the countermeasures in the GDT components which are interrelated and dependent on the social, industrial and organization environment, is needed to successfully combat online fraud. The influence of the environment on the countermeasures may have to be exploited through the activities in each environment (see Figure 2) for success. Future research might also look at online fraud in similar emerging nation's contexts, drawing on the revised GDT framework for inspiration.

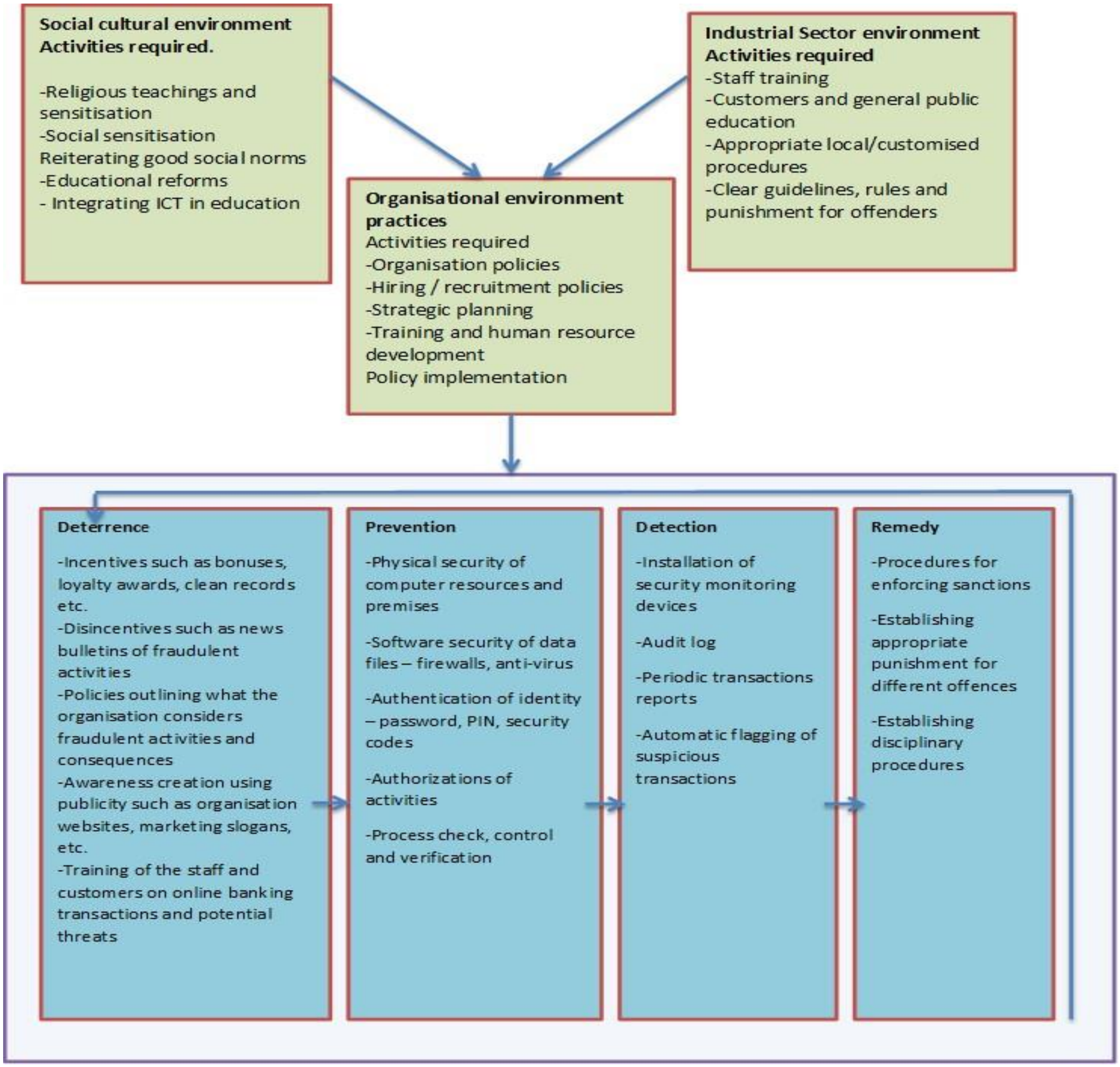
Social cultural environment Activities required.
-Religious teachings and sensitisation
-Social sensitisation
Reiterating good social norms
-Educational reforms
- Integrating ICT in education
Industrial Sector environment Activities required
-Staff training
-Customers and general public education
-Appropriate local/customised procedures
-Clear guidelines, rules and punishment for offenders
Organisational environment practices
Activities required
-Organisation policies
-Hiring / recruitment policies
-Strategic planning
-Training and human resource development
Policy implementation
Deterrence
-Incentives such as bonuses, loyalty awards, clean records etc.
-Disincentives such as news bulletins of fraudulent activities
-Policies outlining what the organisation considers fraudulent activities and consequences
-Awareness creation using publicity such as organisation websites, marketing slogans, etc.
-Training of the staff and customers on online banking transactions and potential threats
Prevention
-Physical security of computer resources and premises
-Software security of data files – firewalls, anti-virus
-Authentication of identity – password, PIN, security codes
-Authorizations of activities
-Process check, control and verification
Detection
-Installation of security monitoring devices
-Audit log
-Periodic transactions reports
-Automatic flagging of suspicious transactions
Remedy
-Procedures for enforcing sanctions
-Establishing appropriate punishment for different offences
-Establishing disciplinary procedures

Figure 2 GDT: Online fraud proposed model/framework

Conclusion

Based on the cultural and social background of people, the perception of online fraud has not helped create necessary awareness or deterred and prevented fraud. There is need to change the orientation and perception of the people and create more awareness through training and publicity of possible threats of attack and fraud. However, social-cultural, industrial environment and organizational environment practices have a strong impact on the four components; deterrence, prevention, detection and remedy. This model, the GDT, it is hoped will help to combat online fraud, particularly in Saudi Arabia.

References

Ahmed S., Buragga K. & Ramani A.K. 2011. "Security issues concern for E-learning by Saudi universities", ICACT Feb. 13-16.

Albert, M. R. 2002. "E-Buyer beware: why online auction fraud should be regulated," *American Business Law Journal, (*39:4), pp. 575-644.

Alfuraih S.I. 2008. "E-commerce and e-commerce fraud in Saudi Arabia: A case study," in *Proceedings of 2nd International Conference on Information Security and Assurance (ISA 2008)*, pp. 176-180.

Attride-Stirling, J. 2001. "Thematic networks: an analytic tool for qualitative research," *Qualitative Research,* (1:3), pp. 385-405.

Braun, V. & Clarke, V. 2006. "Using thematic analysis in psychology," *Qualitative Research in Psychology,* (3), pp. 77-101.

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

Brytting T., Minogue R., & Morino V. 2011. *The Anatomy of Fraud and Corruption*, Kindle Edition, p. 294.

Buller, A. 2012. *Biggest Banks In Saudi Arabia*, http://gulfbusiness.com/2012/08/top-banks-in-saudi-arabia. [Last accessed 17 April 2014]

Chen, Y., Ramamurthy, K., and Wen, K.-W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), Winter2012, pp. 157-188.

Corbin, J. & Strauss, A. 2008. *Basics of Qualitative Research; techniques and procedures for developing grounded theory*, 3rd edn, SAGE, CA.

Creswell, J.W. 2007. *Qualitative inquiry and research design: Choosing among five traditions* 2nd edn, Sage, Thousand Oaks, CA.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research* (20:1), pp. 79-98.

Deloitte, 2011. *GCC Fraud Survey 2011 - Facing the Challenge of Fraud.*

Dwyer, P. C. 2010. *Cyber Crime in the Middle East*, http://www.paulcdwyer.com/Cyber Crime in the Middle East - PCD.pdf. [Last accessed 28 February 2014]

El-Guindy M.N. (2008), "Cybercrime in the Middle East," *ISSA Journal*, June.

Hawkins S., Yen D.C., and Chou D.C. 2000. "Awareness and challenges of Internet security," *Information Management & Computer Security* (8:3) pp. 131-143.

Hennink, M., Hutter, I. & Bailey, A. 2011. *Qualitative Research Methods,* SAGE Publications Ltd, London.

Internet Crime Complaint Center (ICCC), 2010. *Internet Crime Report*, p. 18.

Jing, F., and Pengzhu, Z. 2011. "Study on e-government information misuse based on General Deterrence Theory," *8th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1-6.

Karake-Shalhoub, Z. and Al Qasimi, L. 2003. *The UAE and Information Society*, report prepared for ESCWA, United Nations and presented in February at United Nations, Geneva.

Kotulic, A. G. and Clark, J. G. 2004. "Why there aren't more information security research studies," *Information & Management,* (41:5), pp. 597-607.

Lapadat, J. C., & Lindsay, A. C. 1999. "Transcription in Research and Practice: From Standardization of Technique to Interpretive Positionings," *Qualitative Inquiry, (5:*1), pp. 64-86.

Martin, E. (ed.) 2003. *Oxford Dictionary of Law*, 5th edn. Oxford: Oxford University Press.

Montague D. 2011. *Essentials of Online Payment Security and Fraud Prevention*, John Wiley & Sons, Inc. Hoboken, New Jersey.

Myers, M. 2009. *Qualitative Research in Business & Management*, Sage Publications, London.

Patton, M. 1990. *Qualitative Evaluation and Research Methods,* 2nd edn, SAGE, Newbury Park.

Riessman, C. K. 1993. *Narrative Analysis*. Newbury Park, CA: Sage.

Samociuk M., Iyer N., Doody H. 2010. *A Short Guide to Fraud Risk*, Gower; 2nd edn.

Straub, D. W. and Welke, R. J. 1998. "Coping with systems risk: security planning models for management decision making," *MIS Quarterly,* (22:4), pp. 441-469.

Wells, J. T. 2010. Internet Fraud Casebook: The World Wide Web of Deceit, John Wiley & Sons, New Jersey.

Whitman, M. E. 2004. "In defence of the realm: understanding the threats to information security," *International Journal of Information Management,* (24:1), pp. 43-57.