R Barker

Managing online crisis-communication response in a South African bank: a comparative analysis

ABSTRACT

Deregulation and rapid growth in technology removed entry barriers in the online environment, thereby forcing financial institutions to transform and at the same time to conquer consumer's fear and the perceived risk of fraudulent online transactions. Given the nature of operations and services in the banking sector, it is relatively amenable to innovative technologies, especially online banking transactions. Various studies have been conducted on the adoption of self-service technology, specifically the continued use of this technology, perceived risk in online transactions, and also purchase intention. However, very little research has examined the management of online crisis-communication response messages in the online-security sphere. The *knowledge management* paradigm constitutes a way in which the acquisition, transfer and assimilation of information can be effectively used to manage and control messages in an online crisis-communication response situation, in particular through maximising consumers' motivation and capability to act in response to perceived online-transaction risks. Hence, it provides a means of reliance upon self-motivation and empowerment of individuals to ensure output control and the safety of online banking transactions. The aim of this paper is to present a comparative analysis of the knowledge management of online crisis-communication response in respect of fraudulent banking transactions in one of the top ten banks in South Africa during two specified time periods. The paper first presents a synopsis of the theoretical underpinning based on an extensive literature review. The latter focuses on web communication, online crisis-communication response, fraudulent banking transactions and knowledge management. The methodology, data analysis and results are subsequently presented. Finally, a discussion of the main results based on the knowledge-management typologies proposed to manage and control messages in online crisis-communication response is presented.

Prof Rachel Barker lectures in the Department of Communication Science at the University of South Africa (UNISA).

INTRODUCTION

The ability to do online banking transactions and the interoperability thus created is not only a prism of technological innovation, but has also unlocked opportunities for online crisis communication, an impeding factor raising security concerns related to Internet banking. Internet banking encompasses a whole range of banking services that can be accessed tenuously with the use of an Internet browser and, as a result, creates various enticements to use it. In spite of the appeal to use it, limited research has been conducted on the management of information on the Internet during crisis communication response. Some research has analysed how the use of other online communication tools like interactive chats, real-time video or audio files can be used in crisis communication (Gonzàlez-Herrero & Smith, 2008: 144). These considerable innovations open up the possibility for fraudulent transactions, which presents tremendous challenges to the banking sector to manage online crisis-communication response in that consumers may not accept this service because of fears or discomfort (Lin & Hsieh, 2006) or of security concerns (Barker, 2009; Polasik & Wisniewski, 2009). Furthermore, a basic concern should be to ensure consumers that their electronic transactions are protected against fraudsters who are becoming more and more sophisticated and erudite with clever scams. Hence, Aggelis (2006) argues that banks should optimise the use of reliable detection systems to investigate any ‘strange’ online banking transactions. A study conducted by Campbell and Frei (2010: 4) evidenced that the consequences of adopting online banking can, inter alia, be associated with higher customer retention.

A number of researchers point to the lack of research on online crisis communication. For example, Greer and Moreland (2003: 428) state that “research is scarce regarding the use of online communication following a major incident”. Conway, Ward, Lewis and Bernhardt (2007: 213) contend that the Internet has “the ability to instantaneously distribute information to and is a powerful basis for Internet potential crisis to protect the reputation of an organisation”. Barker (2009) argues that a crisis can become a time of chaos, risk and uncertainty to companies that require timely and appropriate communication to minimise damage to the company’s reputation and also to maintain consumer trust. Despite the advantages of the Internet, organisations will have to realise that this ‘online-security-sphere’ is going to continue to explode, thereby opening up more and more challenges to manage and control it in future.

Consequently, this paper intends to provide a comparative analysis of the knowledge management of messages before, during and after online crisis-communication response based on the websites content dedicated to online security and fraudulent transactions in one of the top ten banks in South Africa during two specified time periods. Specifically, the study is a continuation of previous research conducted by Barker (2009), which focused on the way in which knowledge management, through change agents or online crisis-communication ‘experts’, can have a positive effect on how online banking transactions messages are managed proactively before, during and after online crisis-communication response.

1. KEY CONCEPTS

The key concepts of interest to this study are as follows:

1.1 Online communication

Online communication, like the Internet that is a communication medium possessing the ability to impart information instantaneously to preponderance consumers (Conway, Ward, Lewis & Bernhardt, 2007), offers organisations the opportunity to build relationships with their consumers and stakeholders. It can also be used to offer diverse information on a variety of organisational information and services. Despite the growing importance of and the realisation that online communication messages should be managed before, during and after crises to correct misinformation, research found that websites are limited in terms of communication with consumers and employees during a crisis (Greer & Moreland, 2003). This study therefore focuses on the management of messages in online communication, specifically the Internet.

1.2 Online crisis-communication response

Online crisis-communication response refers to the use of the Internet as an effective online communication device or tool to respond adequately to crisis by providing immediate customised and personalised delivery of interactive messages based on consumer needs in the event of a crisis (Barker, 2009). It is argued that, in reality, effective online crisis-communication response can assist management to face the additional litmus test of the amount of negative attention online crises receive and ensure that organisations are not reluctant to embrace online security issues. Various authors emphasise the importance of immediate response during a crisis. Anthonissen (2009), for example, argues that the response of an organisation and the appropriateness of the response is crucial to the reputation of the organisation, whilst Greer and Moreland (2003) suggest that effective [online] crisis communication response requires customised content-based messages appropriate to the level or stage of the crisis and the needs of consumers.

For the purposes of this study, it is argued that online crisis-communication response to a crisis should be proactive, accurate and open with all stakeholders on the corporate website so as effectively to enable the organisation. Although the literature proposes various strategies for use in a crisis response – including attacking the accuser, denial, excuse, justification, ingratiation, corrective and/or full apology (MacLiam & Barker, 2009; White, 2009) – this study focuses on the knowledge management of messages through an agent or expert to address the demand for information during online crisis-communication response (Barker, 2009).

1.3 Online banking transactions

The Internet permits consumers to, inter alia, take on and engage in online banking transactions. According to Andrews and Boyle (2008: 60), the main inhibiting factor for many forms of online transactions is one of perceived risk, especially in Internet banking, which influences consumer's perceptions and behaviour either to adopt or reject such online transactions. This type of perceived risk is defined by Sathye (1999: 326) as "the security and reliability of transactions over the Internet"; moreover, the risk of losing money through fraudulent transactions or that personal information might be misused (Drennan, Sullivan, Mort & Previte, 2006).

Depending on the predefined perspectives of the researchers on the particular context under scrutiny, there could be various viewpoints regarding perceived risks. In line with the declared purpose of this paper, i.e. to examine the management of messages proactively during online crisis-communication response, the focus will here be on management of knowledge either to prevent or address fraudulent banking transactions when they actually do occur.

2. ADVANTAGES AND DISADVANTAGES OF ONLINE OR INTERNET BANKING

Much has been written on the multitude of benefits the Internet offers to users and providers. Various studies have been conducted on the positive impact of online service provision on banks' performances (DeYoung, 2005; Hasan, Zazzara & Ciciretti, 2005; Hernando & Nieto, 2007). Yet, for various reasons, some consumers are still reluctant to use this service.

Table 1 provides a brief summary of the main advantages and disadvantages of online banking identified by various researchers (DeYoung, Lang & Nolte, 2007; Gan, Clemens, Limsombunchai & Weng, 2006; Hernando & Nieto, 2007; Lee, Kwon & Schumann 2005; Mannan & Van Oorschot 2007; Polasik & Wisniewski, 2009).

Table 1:Advantages and disadvantages of online or Internet banking

Advantages	**Disadvantages**
Low cost, currently the cheapest distribution channel for standardised bank operations (such as account services, payments or transfers)	Security concerns can dampen enthusiasm of potential users
Alternative distribution channel to increase bank revenues by selling additional fee-based services	Powerful basis for online crisis potential, which could harm the reputation of the organisation's services and brands
Reduction of overhead expenses, specifically costs related to maintenance of physical branches, marketing and labour	Problems experienced by consumers regarding unauthorised transactions

Can serve more consumers and provide access to consumers residing outside the branch networks	Lack of Internet or computer access by consumers and rapid development of IT.
Creates opportunities for effective cross-selling	Availability of broadband is limited, especially to rural areas
Consumers are motivated by convenience and efficiency and online banking reduces physical visits to the bank	Income levels and other demographic characteristics are important predictors of the adoption status
Incentives such as lower fees or better rates on deposits and loans because of increased competition	Exploitation of the convenience and the overhead savings
Consumers feel they have better access to information, speed of payment transactions or a sense of control over transactions	Consumers may be averse to the idea of online banking because of either low educational levels or the unavailability of adequate information about the distribution channel
Opportunity to educate consumers on safe and secure online banking	Fear of scams, hacking attacks and identity theft and of attracting criminals who exploit consumers

3. LITERATURE REVIEW

Limited research has been conducted specifically on the management of online crisis-communication response before, during and after a crisis. The theoretical perspectives that were the focus of previous studies on crisis communication theory can be divided into three main categories: chaos theory; excellence theory and knowledge-management theory (Barker, 2009; Grunig & Grunig, 2002; Lueg, 2001; MacLiam & Barker, 2009; Swart, 2010; Verwey, Crystal & Bloom, 2002:31).

- *Chaos theory* is a derivative of systems theory and refers to the attempt to understand the behaviour of systems that follows unconventional or irregular paths yet display certain patterns over time. The application of chaos theory to crisis studies is possible in that similar dynamics are evident when if a crisis forms a series of events that gains momentum over time and develops into an eventual disordered state. Furthermore, crises do not follow a linear path; they are unpredictable and sometimes occur without warning. Chaos theory assigns a crisis management responsibility to everyone in the organisation – as opposed to the application of a separate crisis team – and thus reflects the incorporation of the organisation as a whole. Chaos theory also regards crisis management as a predominantly proactive and reactive process, through the incorporation of planning (preparation) and reactive (areas of unpredictability) measures. Yet there is insufficient emphasis on evaluating crisis occurrences or on incorporating these lessons in order to assist the organisation to avoid a similar crisis in the future.

- Most crisis-communication theory builds on Grunig and Grunig's excellence model (2000) grounded in different approaches to public relations practice ranked hierarchically in relation to their potential for excellence, of which the two-way symmetrical model has been used successfully by many as a solution to successful crisis communication. Excellence theory evolved from the search to determine how public relations should be practised and the communication function be organised in order, inter alia, to contribute to *organisational success*. It highlights the *monetary value* of public relations to the organisation, building sustainable relationships with strategic constituencies and public relations *effectiveness*.
- More recent crisis-communication perspectives are grounded in the *knowledge-management paradigm*, which is seen as a multifaceted socio-technical process encompassing various forms of knowledge creation, storing, representation, and sharing to the benefit of the organisation and its individuals. It is seen as information with specific properties and the introductory stage to knowledge. From a crisis-communication response perspective, three key components of the knowledge management process have been adapted for the purposes of this study: a *technical* component (data gathering, mining and knowledge construction); a *communication* component (knowledge creation and sharing of information through online messages during direct, real-time interactions); and a *human* or organisational component (management of four interrelated elements, namely choice, adoption and implementation of procedures/methods to link individuals and groups; formal and informal informational settings in which interaction occurs; organisational practices to address the crisis, and the context in which interactions and messages are facilitated).

Given the criticism of and "*growing scepticism towards the 'idealism' of two-way communication*" (Fjeld & Molesworth, 2006) – mainly because of its complexity and the fact that communication in the virtual environment is mostly one-to-many and many-to-many allowing for speed, global reach and the covering of crisis in real-time – it is argued that the knowledge-management paradigm allows organisations to reach consumers directly without messages being filtered, which signifies the significance of managing and controlling online messages. This is in line with arguments advanced by Gonzàles-Herrero and Smith (2008: 145). They state that, on the one hand, the Internet acts as a 'trigger' caused by rumours, hacking, copycat websites, websecurity breaks and all forms of cyber-terrorism/cybercrooks. On the other, it serves as 'facilitator', i.e. an agent that accelerates messages on the crises to provide a new dimension for proactive online crisis-communication response through knowledge management.

Barker (2009) accordingly argues that despite a tendency to follow the tradition of thinking of communication as the transfer and processing of information, the current state of affairs tends to focus on the proactive management of *messages* through knowledge creation and knowledge sharing. One of the key discourses of the knowledge-management paradigm is that embodied, tacit, implicit and narrative knowledge are important phenomena and fundamental to all human knowing (Nonaka & Takeuchi, 1995). Moreover, these kinds of knowledge are essential parts of everyday communication because they allow for the transformation, sharing and processing of knowledge (Barker, 2008). If applied to online crisis-communication response, it is argued that the knowledge management paradigm offers a means of managing messages that are *acquired, transferred and assimilated* before, during and after a crisis (Barker, 2009).

The continuing point of this article is therefore evidenced in the applicability of knowledge management as a comprehensive approach to crisis management in general, and in this paper particularly with regard to the online crisis-communication response process. In terms of the theoretical discussion of the knowledge-management paradigm, the following three key online crisis typologies are prevalent (Barker, 2009):

- Acknowledge the crisis and *acquire knowledge* through data mining and knowledge construction to address it proactively (whether empathic, warnings against complacency, addressing ambiguity and uncertainty, etc.).
- Adequate response and attitude towards the crisis by means of *transfer of knowledge* to consumers through the creation and sharing of knowledge in direct real-time interactions (for example setting the consumers' minds at ease, ensuring them of the safety and security of online transactions, etc.
- *Assimilation of knowledge* to address those affected by the crisis and to present methods and procedures to link consumers to possible preventative or corrective actions to ensure authenticity and transparency in the trust-building process (for example through downloading of free software, steps or guidelines to ensure safe and secure use of online transactions, reduced risk strategies, etc.).

Subsequently, for the purposes of this study, it is argued that online crisis-communication response should incorporate three aspects of the crisis-management process as highlighted by Swart (2010): proactive planning and preparation of the organisation for possible crisis situations; sufficient and prompt response to crises; and employing post-evaluative actions in order facilitate learning and prepare the organisation for future crisis events.

The application of the key typologies during online crisis-communication response on the website is indicated in Figure 1, followed by a brief delineation of each.

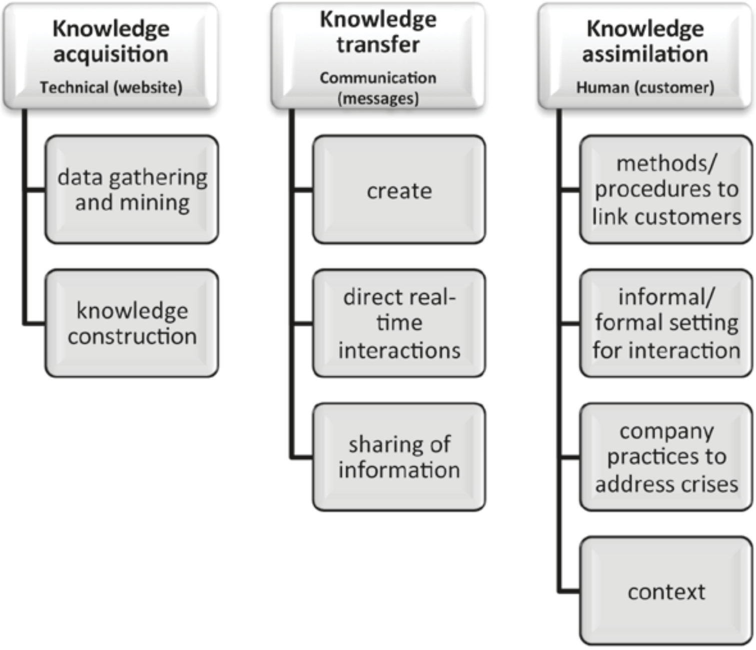

Figure 1: Mapping of the knowledge-management process during online crisis-communication response (Barker, 2009)

Each of these typologies can be briefly recapitulated as follows (Barker, 2009; Elliot, 2009).

- **Knowledge acquisition:** It assists with the creation of the enabling messages to steer the online crisis-communication response of an organisation. Based on the knowledge management paradigm, this refers specifically to the technical component (in this case the website used for online crisis communication), which focuses on the gathering of information through data mining and knowledge construction.
- **Knowledge transfer:** In this process, communication messages are created to ensure direct real-time interactions to facilitate the effective transfer and sharing of information. Such messages are imperative towards translating explicit knowledge into tacit forms that can be understood by the consumer; hence, this refers to the communication component.
- **Knowledge assimilation:** During this stage, informal and formal systems and practices should be integrated, existing methods and procedures should link consumers to other websites, and practices should be in place to address and/or prevent a crisis. Furthermore, it is suggested that an agent or expert should be included in the knowledge-management process to contextualise and manage messages to the consumer, thereby addressing the human component.

Theoretically, analysis of online fraudulent transactions has demonstrated that the verified key rudiments of online crisis-communication response are proactively to provide informational messages by providing facts; to indicate how consumers should or should not act; and, to present information on how the crisis can/has been corrected or not. It is hence asserted that the knowledge-management paradigm propounds the opportunity to manage online crisis-communication response by means of these typologies, through a succession of messages and links, to assure consumers of safe and secure online transactions.

4. RESEARCH METHODOLOGY

This study utilised a *qualitative content analysis* of websites on fraudulent transactions and safety and was based on typologies derived from a comprehensive literature review. Building on the knowledge-management paradigm, online crisis-communication theory and the use of the Internet for online banking transactions, this study presents a comparative analysis of data collected and analysed on the management and control of messages before, during and after incidents of fraudulent online banking transactions. This study empirically tested the data collected based on the typologies of the knowledge management paradigm through a comparative analysis of two specified time periods.

The bank, which was the unit of analysis, was one of the leading educators in the area of online banking in South Africa, specifically because of the proactive online communication and messages on fraudulent banking transactions, possible security threats and corresponding precautions to avoid similar incidents of crisis. The data were gathered by accessing the websites of the bank in the time periods July 2006 to July 2009 (when online fraudulent transactions became and were most prevalent and their management was both reactive and proactive) and July 2009 to July 2010 (mainly to manage online messages through proactive actions). Available and accessible pages primarily associated with information about the online banking transaction crisis and/or the security and safety of online transactions were printed during these time frames. The printed *material* included any special fraudulent banking transaction, crisis-specific pages, and information from regular web pages that contained links to the crisis. In order to determine the cumulative number of crisis-related messages posted by the bank on their websites, the researcher conducted a post-hoc analysis of the sites' contents. Included in the analyses were additions and deletions of individual organisation-generated messages (for example, media releases, fact sheets and messages from the agent or expert) and links to other and/or new sites. From an online perspective, the study set out to conduct a comparative analysis of the indicated time frames to examine the extent to which messages were controlled and managed (whether proactively or reactively) to ensure effective online crisis-communication response.

The qualitative research methodology entailed a case study-based comparative analysis of the online fraud and security-centre website messages of one of the top ten major banks in South Africa. The selection of the bank by means of purposive sampling means that it was conveniently available and prominent in the use of these websites. This specific bank was selected because of ease of access to information, availability of information, permission to use information obtained through data mining, etc., which were absent or not prevalent in the websites of the other banks during the specified time frames. To achieve the aims of the study, it is positioned within a knowledge-management paradigm that acknowledges a relativist online ontology and epistemology (Denzin & Lincoln, 2003; Fuchs, 2009; Goulding, 1999). Ontologically, multiple realities are created and the subjective role of the researcher in the process of constructing and analysing such online realities is an acknowledged attribute of the research. Epistemologically, the researcher seeks to uncover the nature of the agents or expert's experience and interpretation to control and manage the phenomenon of interest and, by means of knowledge management, to interpret it within the reality of online crisis-communication response. Hence, the findings provide a rich and meaningful interpretation of the online banking transactions to present a depiction of the 'real life' situation (Barker, 2009).

Reliability is assessed through construct reliability, in other words the degree to which the observed constructs reflect underlying factors, in this case whether they reflected the identified typologies during both studies. *Internal validity* was attended to by way of consistently evaluating the existing websites during both time frames, while addressing the theoretical concepts under investigation in each study (Barker, 2009). A degree of *discriminant validity* was assured by using conceptually similar concepts distinct to the measures of theoretically different constructs in both studies (Nusair & Hua, 2010: 316). This study also addressed validity in respect of generalisation by using the typologies indicated in Figure 1. These typologies are generally apparent in knowledge management and online crisis-communication response and can be used both in this comparative study and in other, future studies.

5. DATA ANALYSIS AND FINDINGS

5.1 Data analysis

The data analysis of the first study was duplicated by means of an iterative process. This entailed data coding to identify typologies of initial concepts, identifying integrative concepts applicable to all the subjects in the study and by selective coding to reduce these to emergent themes. An inductive approach was used to report on the findings based on descriptions and interpretative comments relating them to and drawing on the key theoretical concepts and thrusts identified for the purpose of the study (Barker, 2009).

The comparative analysis reflected on data obtained during the two specified time frames, namely July 2006 to July 2009, and July 2009 to July 2010, assessed online through the website.

The typologies identified in Figure 1 were assessed through the concept lurking where the researcher was a non-participative observer trying to understand the meaning transferred to the consumers through the three components (technical, communication and human) of the knowledge-management paradigm (Barker, 2009). Evans, Wedande and Van 't Hul (2001: 154) explain lurking as a way for the researcher, staying in the background, to become familiar with the rules or norms of a community with a view to understanding and establishing the implied meaning of the messages and subject matter before making a contribution in virtual communities. Because online websites have an idiosyncratic voice and community style, the researcher was sensitive towards passivity, vagueness and abbreviations based on observed knowledge of the communication to the consumers (Barker, 2009). Non-participative 'lurking' allowed the researcher to gather relevant information and come up with methods to try to understand the online communication of the 'experts'.

The collected data were coded and analysed using the qualitative data presentation and analysis methods proposed by Miles and Huberman (1994). These include development of summary sheets, coding of the online websites on fraudulent transactions in terms of the theoretical paradigms identified for the study, weighting of the specific criteria, and, coding of the overall data.

The main links and sub links illustrated in Table 3 were used for the comparative analysis of the three theoretical typologies derived from the literature reviews and the components used to evaluate and measure the descriptions in the websites on fraudulent transactions by means of lurking. For example, the typology *knowledge acquisition* was measured by comparing the assumed knowledge construction through data gathering and mining construction on the website (technical component) during the two specified time frames. Another example is that the typology *knowledge transfer* was differentiated both in terms of the creation of observed direct real-time interactions and also of the sharing of information through messages (the communication component). Similarly, the final example was drawing a distinction in terms of the typology *knowledge assimilation*, which was measured by means of the methods/ procedures to link consumers, informal/formal setting for interaction and organisation practices to address crisis to the consumer (human component). A comparative analysis was also conducted to reflect on the main links and sub links to the security centre on the website as indicated in Table 2.

5.2 Findings

The monitoring of the websites resulted in the following message constructions of fraudulent transactions categorised/identified by the researcher (indicated in Table 2):

Table 2: Message construction of fraudulent transactions of bank

Message construction of fraudulent transactions (categories on fraud)	Time Frame 1: July 2006-2009	Time frame 2: July 2009-2010
Media releases	25	3
Online fraud updates/messages from 'expert'	5	10
Links	30	45

These results are graphically presented in Figure 1.

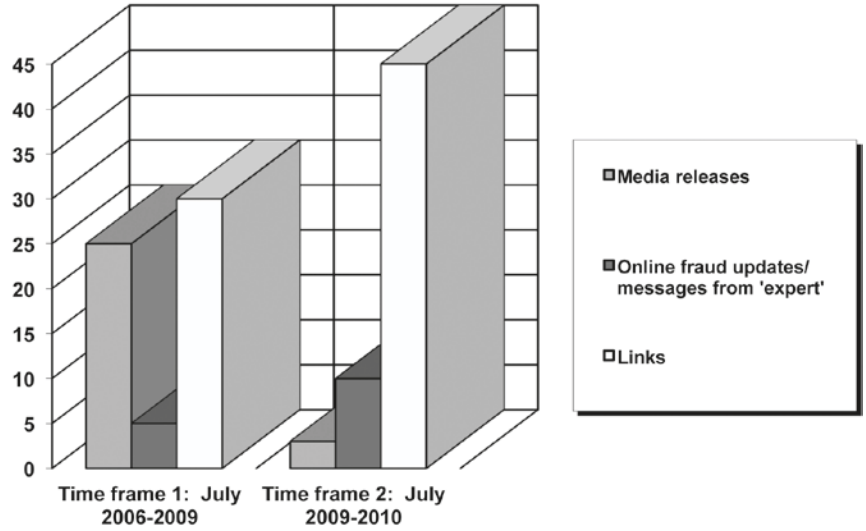

Figure 2: Message construction of the bank's fraudulent transactions

Comparative analysis of the three message-construction formats listed in Table 1 and graphically presented in Figure 2, yielded the following results:

5.2.1 Media releases

Evaluation of these particular message constructions revealed that in the first time frame, the 25 media release postings on the website focused mainly on the following types of message postings:

- General security information (1)
- Security software – free downloads (4)
- Security warnings – for example, SIM swap, Nigerian 419 or 'advance fee' fraud, phishing, card skidding, pin number, etc. (10)
- Safety tips (5)
- Security measures – like 'jittering cards' for safety (5)

In the second time frame, messages on security issues were limited to warnings on fraudulent transactions, specifically 'Beware of hoax emails', 'phishing' and MyDoom email viruses (5). Although various media releases were released during Time Frame 2, only three media releases specifically addressed fraudulent banking transactions, focusing on the security warnings, for example warnings against hoax emails (3).

Another interesting observation was the fact that of the 301 media releases archived since 2005, 25 covered security-related messages on online fraudulent actions during Time Frame 1, and only three during Time Frame 2.

5.2.2 Online fraud updates/messages from the 'expert'

The increase in the number of 'updates or messages' from the expert in Time Frame 2 are attributable to the fact that knowledge was managed proactively, before the crisis, by the 'expert' who ensured that consumers were knowledgeable and informed about the possibility of crises, thereby supporting the argument that doing so would eradicate the need for reactive approaches. This is evidenced in the fact that many of the messages in the previous media releases during Time Frame 1 – like 'Nigeria 419' and 'Latest E-mail Scam – card holders' – had a specific link on the security centre under 'Archived Articles' to address the previous type of scams. It can thus be seen as proactive knowledge management by 'experts' in the bank to prevent online crisis response.

5.2.3 Links

The results of the comparative analysis clearly indicate that a number of links were added during Time Frame 2, while this had not been the case with Time Frame 1. Again, this emphasises the fact that knowledge is managed proactively and that various links are available to share and create meaning and to disseminate these to consumers.

In terms of the *typologies of knowledge management*, the notable differences evident from the main findings of the comparative analysis are summarised in Table 3.

Table 3: Data analysis in terms of the typologies of knowledge management

Typology	Components/ criteria	Time Frame 1: July 2006-2009	Time Frame 2: July 2009-2010
Knowledge acquisition	Technical (website): • data gathering and mining • knowledge construction	Security Centre website – privacy prominent on website Detailed links to broad spectrum of fraud and safety measures Messages constructed based on existing data	Security Centre website very prominent – prompt to read safety measures and click *OK* that it has been read Site privacy also prominent on website More detailed links to cover broad spectrum of fraud and safety measures, including archived information Messages constructed based on existing data – regularly updated and very detailed
Knowledge transfer	Communication (messages): • create • direct real-time interactions • sharing of information	Communication via the creation and sharing of detailed messages through direct real-time interactions on home page Real examples of scams through the following: • useful links • security link on *Consumer Service and Charter* • electronic banking solutions Detailed messages created Sharing of information through examples of fraudulent emails and direct real-time interactions	Communication via the creation and sharing of detailed messages and various specific links through direct real-time interactions on home page Real examples of scams through the following: • 3D secure • About security • Antivirus software • Fraud squad • Digital certificates • Internet banking • Scams • Security tips • Virus watch • Archived articles Detailed messages and examples created Sharing of information through examples of fraudulent emails and direct real-time interactions

Knowledge assimilation	Human (consumer): • methods/ procedures to link consumers • informal/formal setting for interaction • organisation practices to address crisis • context	Home page includes warning about fraudulent transactions Prominent links for consumer to Security Centre Online fraud update with regular online fraud updates (e.g. *Beware, don't be caught; please check account*): • Latest scams • Security tips • Virus watch • Fraud squad • Antivirus software General security messages in informal and formal settings Detailed methods, practices and procedures provided to consumers to ensure security in informal and formal settings Clear indication of the bank's practices to address fraudulent online transactions both proactively and reactively Clear contextualisation of messages	Home page includes warning about fraudulent transactions Prominent links for consumer to Security Centre Online fraud update: • Search engines • Online Applications • Firewalls • Antivirus software • Fraud squad • Digital certificates • Internet banking fraud: warnings about the following: Internet-banking security measures; Internet-banking precautions (Account no and password); secure site questions; certificate, VeriSign, security features, information for Internet Explorer users; privacy settings, how to check Internet-banking security; RVN (Random verification number) • Internet-banking fraud • Internet-banking security measures • Scams • Security tips • Virus watch • Archived articles on previous security articles General security messages in informal and formal settings Detailed methods, practices and procedures provided to consumers to ensure security in informal and formal settings. Clear indication of the bank's practices to address, both proactively and reactively, fraudulent online transactions Clear contextualisation of messages – more detailed and more examples than in first time frame

The results of the comparative analysis between the main links and sub links of the messages on the websites during the two specified time frames are graphically depicted in Figure 3 on the next page.

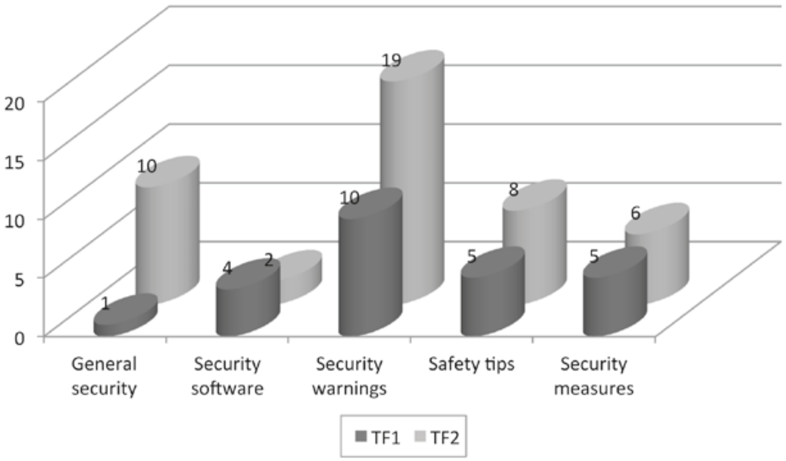

Figure 3: Main links and sub links of messages on the security websites

In the analysis of the knowledge management of messages in terms of the typologies of knowledge management either to address or prevent fraudulent online banking transactions and also in terms of the main links and sub links of messages on the security websites, the comparative analysis provided the following contributions and points of discussion.

In the first time frame when fraudulent banking transactions were at their height, it was clear that preference was given to posting online messages to inform, educate and make consumers aware of potential fraudulent actions and security measures on a constant basis, both proactively and reactively. In addition, various main links and sublinks were created and posted on the websites. The results indicated that the security and privacy requirements and measures on the bank's websites during this time frame were of great importance and received prominent coverage. During the second time frame, the bank's security measurements for online banking also comprised passwords, anti-malware, up-to-date operating systems, etc. as was the case in the first time frame). However, the main links and sub links of messages were much more comprehensive including in that they included examples of the latest scams, warning (Important notice) pages, which came up when one logged on to the website, transaction verification numbers, 3D-software, firewalls, to name but a few. This is indicative of the three key typologies of the knowledge-management paradigm, i.e., that the bank achieved extremely high scores on all counts and that most of the criteria of each typology of the knowledge-management paradigm were adhered to. Furthermore, it was clear that, because of the proactive control and management of messages, consumers were assured through various means that online transactions were safe and secure. Within each of these typologies, the 'expert' initiated messages to react, warn and update consumers (proactively and reactively) and included real-time examples of fraudulent emails and scams. The messages were made available quickly and immediately after incidents of fraudulent banking transactions became evident (whether through the media, emails or the website). They were factual, and assured consumers that security and safety measures were being applied by the bank on a continuous basis. This is in line with the arguments based on the literature review, namely that initial response to a crisis should be quick, consistent, open, sympathetic and informative. Furthermore, one main link to the Security Centre created in Time Frame 1 was moreover still evident on the home page during the second time frame, although much more information and many more links were created – mostly proactively. The Security Centre during the first time frame had 10 main links to security issues ranging from downloading free software to security tips and scams. The latter included four sub links related specifically to scams (email scam, payment confirmations, online fraud update, and the latest cell phone identity scam). In Time Frame 2, there were 47 such links. Also, one link to security was evident on the Consumer Service and Charter web page throughout both time frames.

The opening page of the bank created during Time Frame 1 continued to indicate a message on potentially fraudulent transactions and security messages to inform customers on actions to be taken to ensure safety in the second phase. The website also indicates that they initiated online responses specifically to *disseminate information* about the crisis. The postings included a *special page* that users saw when they opened the online web page. It informed the customers of possible fraudulent online transactions with instructive communication on how to respond and adhere so as not to become a victim. Furthermore, more *links* to the *security* website were established than there had been during the first time frame, with detailed information on possible schemes and information as to what to do – this being mainly indicative of a *proactive approach*. In the second time frame, the media releases sent out in the first time frame were accumulated under 'archives' for purposes of *data mining* and *storing*.

The key differences between the online crisis-communication responses in the first and the second time frame was probably the fact that the bank was much more consistently *proactive*, *used informative messages*, included statements to assist victims, provided toll-free phone numbers, assuring them that online banking was safe and secure. In contrast, where the bank mainly responded reactively in Time Frame 1, especially in the beginning when online fraudulent actions in online banking were more prevalent and most information was centred in media releases and postings, the bank responded more proactively with more main links and sub links established on the website during Time Frame 2. Differences also existed in the *frequency* with which information was released. During the first time frame, messages were more frequent and more media releases were issued, whilst in the second time frame the data collected during the first time frame were structured clearly with visible links to prevent rather than address online fraudulent transactions.

A further difference lay in the *initial and follow-up* responses. Although the bank initially featured various security messages when consumers accessed the site, the bank added a number of links to connect customers to its security website during the second time frame, which included information on new scams and security measures/software. Where the bank in the beginning mostly responded by adding media releases representing a mix of operational and personal information, they later featured announcements regarding possible fraudulent transactions and provided information to customers on preventative actions. One feature unique to the bank's knowledge management in the second time frame was the addition of the security message that popped up when consumers logged into their account where they had to confirm that they had read the security methods and procedures and that they were knowledgeable about the content. This is an excellent example of how security issues are managed *proactively* by an expert or from the web agent.

The features of the main links and sub links also differed considerably. For example, during the first time frame, the bank focused mainly on messages to address the crisis reactively by providing general security information, security software – free downloads, security warnings – for example SIM swap, Nigerian 419 or 'advance fee' fraud, phishing, card skidding, pin number, etc., safety tips and security measures – like the jittering cards for safety with more reliance on the data available on the website later in this time frame. During the second time frame, messages focused more on the proactive management of messages and contained a general description of the types of crisis that could be expected, and also a description of the bank's assistance methods and program. The bank moreover assured customers by means of statements and links through which they could access additional information on what was expected of them. Most of this information also featured on the website with various links, thus offering multiple connections from dual locations on the website.

Another issue identified in the literature was *interactivity*. The bank's website seemed to be lacking in this area, particularly in relation to fraudulent transactions. Although contact details, through a toll-free telephone number, were in fact indicated, it was possible, on the one hand, that the lack of interaction was attributable to the potential for information overload at call centres after a crisis. On the other, proactive knowledge management minimised potential crisis and the need for interactivity. This correlates with the issue, identified in the literature, of the importance of *direct real-time interactivity*. The website of the bank in the study seemed to be prominent in this area, particularly in relation to fraudulent transactions. Because the study only focused on website content, the bank's interaction with consumers by means of the hotline or toll-free telephone number could not be assessed. In this case, the possibility of a lack of interaction could have been attributed to the potential for information overload at call centres after a crisis.

A further distinction lay in the *initial* and the *follow-up responses*. Although the bank continued to feature informative messages from the *expert* – which consumers saw when they accessed the site – various *links* connecting consumers to the banks' security website were evident. In Time Frame 1, there were various responses through media releases (proactive and reactive). These represented a mix of operational and personal information and featured announcements regarding possible fraudulent transactions and provided information to consumers on what to do. One unique feature during Time Frame 2 was the addition of 'hotline messages/online messages' from the web agent or expert to assure consumers. It appeared that the messages were transcribed for posting on the website.

How, in the first time frame, the bank used its website before, during and after (*in the pre, present and post stages*) the initial crisis is also noteworthy. Generally speaking, the opening page of the bank website not only reflected immediate and proactive reaction, but also provided similar information before, during and after the crisis (either through message construction based on existing data, media releases, statements, online messages, links, etc.), especially within the few days following the crisis. For example, the websites continued to feature both a message on possible fraudulent transactions and security messages to inform consumers on actions to be taken to ensure safety. The website also showed that the expert at the bank initiated online response specifically to disseminate information about the crisis, and the postings included a special page that users saw when they opened the home page and which informed the consumers of possible fraudulent online transactions and provided instructive communication on how they should respond and adhere so as to avoid becoming a victim.

Finally, the most significant change from the first to the second time frame was probably the identification of fraudulent online banking transactions as a possible crisis and also the *proactive measures* that were put in place to manage and control the messages. This was exemplified and evident in a number of messages posted online, which included messages on dealing with online security, media releases to inform customers on safe use of online transactions, statements regarding security requirements and then also new security measures, procedures and operations. That the bank was dealing with the results of the crisis was also evident, and the bank improved the basis format of its website by featuring frequently updated messages and links. Post-crisis communication, the most acute phase, according to Gonzàlez-Herrero and Smith (2008: 151), therefore consistently and proactively introduced new messages about the long-lasting effects of the crisis by managing it effectively.

Interestingly, it was observed that, during the second time frame, a new link, *Site Privacy*, was added. This addressed a wide range of aspects on bank security and policy issues. It featured two sub links, namely *Protecting our Customer* (our commitment to you, our customer; contributing to privacy protection; protecting customer information; sharing customer information; the bank's commitment to customer privacy; Internet-access privacy policy) and *Other Areas of Privacy* (cookies; planning tools; right to amend this privacy statement; privacy statements, e.g. online services, third parties, email communication, and code of banking practices). Emphasis was further placed on the consumer's responsibility both to ensure secure online transactions and to minimise fraudulent banking transactions, specifically by information on 'shared responsibility' during Time Frame 2 – something that was absent during Time Frame 1.

6. DISCUSSION

Analysis of the bank's website during the two specified time frames with a view to analysing the management of messages before, during and after fraudulent online transactions that could result in crises revealed that the content of the sites closely pursued the following three broad crisis-response phases:

- **Action:** Provide instructive information to customers on how to take action when a crisis breaks out through three main types of messages: basic facts about the crisis, providing new information and preparing customers for what to expect and how to react.
- **Adapt/adjust:** Moving into adjusting communication once the immediate impact of the crisis wears off by posting various messages and by linking customers to websites to ensure them of the safe and secure use of online transactions.
- **Abate:** Proactively managing the messages after the crisis has started to fade by internalising content and creating a positive image of the organisation.

Given the above, it is argued that the website messages were organised around the main types of messages identified in Table 1 and when correlated with the typologies set out in Table 2, it is evident that overlaps existed. This in turn indicates that knowledge management can be used as a theoretical point of departure in the managing and control of the different types of messages.

The bank can be said to have been consistently proactive in that it had used frequent informative messages, included factual statements to assist consumers, provided toll-free phone numbers and assured them continuously of the safe and secure use of online transactions.

Finally, the most significant attributes were the identification of fraudulent online banking transactions as constituting a possible crisis and the *proactive measures* that were put in place to manage and control those messages. This was illustrated in a number of messages posted online, e.g. messages on dealing with online security, media releases to inform consumers on the safe use of online transactions, statements about security requirements and new security measures, procedures, practices and operations.

The analysis suggests that the bank complied with the security recommendations and with the three knowledge-management typologies expecting them to keep consumers informed and educated through updated messages managed by an expert. The bank can thus be said to have viewed security as a 'shared responsibility', even if sophisticated and predominantly technical and security awareness/prevention methods might have failed to satisfy online banking requirements (which correspond mainly to the *technological component*). In spite of this, the bank nevertheless urged consumers to maintain ‘security’ by applying specific measures to gain access to online banking transactions, by creating direct real-time interactions and through the constant sharing of mainly proactive information (the *communication component*). The bank furthermore assured consumers that it would not do anything to compromise the security and confidentiality of consumer information. Appeals were also made to the human component by putting methods and procedures in place to link consumers to informal and formal settings for interaction (and immediate feedback) and communicated messages on the organisational practices for addressing crisis in each context.

7. CRITICAL ANALYSIS OF RESULTS

Contextual comparison of the knowledge management during both time frames reveals that the online crisis-communication response in the first time frame was apparently more straightforward in dealing with breaking crises in respect of fraudulent banking transactions, mainly because it started off with a reactive approach and moved towards a proactive approach as more and more information and knowledge were created and shared. Hence the main emphasis was on the typologies *knowledge acquisition* and *knowledge transfer* (to create enabling messages by means of data gathering, data mining and knowledge creation and to ensure direct real-time interactions to transfer and share this knowledge effectively), with a definite move towards *knowledge assimilation* (so as to put formal and informal security systems in place). The knowledge management in the second time frame comprised mainly proactive measures, with a definite focus on *knowledge assimilation*, – especially through ‘expert’ advice – but still addressing the typologies of *knowledge acquisition* and *knowledge transfer*. Knowledge assimilation was evident in maintaining existing methods and procedures and the continuous updating of these with measures to prevent crisis from happening. Knowledge acquisition and transfer were mostly evident and were used to create messages and knowledge to help customers keep abreast with the latest scams and to ensure that proactive measures were put in place.

It is thus argued that in both studies *knowledge acquisition* (the technical component) was, to various degrees, evidenced through the provision of instructive information on the website to consumers for when a crisis broke out. Such information aimed at helping them to take *action* or to prevent a crisis from occurring. This information was obtained not only through data gathering and mining, but also through knowledge construction. Three main types of messages were obtained through data mining and knowledge construction – basic facts about the crisis; updating of existing information and facts; and, provision of new information and messages to prepare consumers for what to expect and how to react to the crisis. This was verified by the establishment of a Security Centre website and of detailed links to cover the broad spectrum and context of fraudulent transactions. *Knowledge transfer* was more apparent in the first time frame with the move into *creating and adjusting* the communication messages once the immediate impact of the crisis wore off by posting various messages and linking consumers to websites for direct real-time interactions and by sharing information to ensure them of the safe and secure use of online transactions. Although examples of possible real-time fraudulent transactions were included on the security websites and the links to transfer this knowledge to the consumer in both time frames, these were more evident and advanced in the second time frame, mainly in respect of proactive measures to ensure online security. *Knowledge assimilation* was substantiated in the first time frame through the management of the messages in the *pre, present and post stages* of the crisis by presenting methods and procedures to ensure safe online banking transactions, by providing informal and formal settings for interaction (for example hotlines and online links), and by stating organisational practices to address the crisis and the context in which it was managed and controlled. This was corroborated by the linking of consumers to the Security Centre, Online Fraud Updates, general security messages (formal or informal), and detailed methods, practices and procedures to address the crisis both proactively and reactively. In the second stage, this was the main typology applied, largely because it was argued that because of an 'expert's' intervention in the first time frame and further to effect knowledge management throughout the crisis, the main emphasis had been on updating and maintaining the methods and measures in a proactive manner.

Consequently, the results echo the strengths of knowledge management during online crisis-communication response in both time frames. The multiple constructs used represented several measures that are distinguished based on whether they are exogenous or endogenous – in this study the constructs acted as independent variables that can simultaneously be interdependent. Furthermore, it is contended that interpretive analysis of the websites in both time frames provides insights into how agents or possible experts can construct messages through data mining to help consumers to compose their own accounts as a lived, direct, real-time experience. Moreover, if these experts are proactive and pay attention to security indicators, such as methods and procedures on websites to reduce perceived risk to consumers during online banking transactions, this reduces the risks of online fraudulent banking transactions.

8. LIMITATION AND CONTRIBUTION OF THE STUDY

The most significant limitation of the qualitative methodology employed here includes a lack of generalisability of findings because of a small, non-representative sample coupled with subjective analysis in that this study was limited to one bank. However, this limitation was largely offset by the comprehensible identified research design undertaken during two time frames – in other words, it was replicated in another study. In spite of the fact that the findings cannot be generalised, it provides the banking industry with measures to gauge proactive knowledge management of online crisis-communication messages, thereby paving the way to reduce perceived risk in fraudulent online transactions.

The main contribution of the study is that it explores arguments for the approval of knowledge management as a plausible theoretical framework that can be applied to online crisis-communication response during fraudulent online banking transactions. This comparative study set the scene for future research. On the one hand, it provides qualitative insights into the importance of knowledge management – through agents or experts – of messages in online crisis-communication response; on the other, it indicates the extent to which reassurance on a website reduces perceived risk for consumers to continue online banking transactions.

9. CONCLUSION

Based on the theoretical typologies derived from the knowledge management paradigm, this paper has focused on a comparative analysis of a bank's management of messages during online crisis-communication response during two specified time frames. It was suggested that the proactive management of messages by means of online knowledge acquisition, transfer and assimilation can avoid, or at least assist in preventing online fraudulent banking transactions.

The significant lesson learnt is that high priority should be assigned to online crisis-communication response when providing online services to consumers. Failure to do so could put organisations at risk and reduce vigilance. A possible solution proposed is to ensure proactive knowledge management of online services so as to address the needs of consumers and possibly to ensure that information security extends to enhancing the reputation of the banking industry as a whole.

Because of a limited number of solutions proposed have to date been to mitigate online crisis communication, this paper presented a possible solution to protect online consumers against fraudulent banking transactions by means of a proactive approach that can be feasible in practice. It is important to realise that fraudulent attacks will remain an important problem for which solutions will constantly be required. In this paper, an extension of a previous study was presented that mitigates shortcomings in existing studies. In particular, this novel approach leverages the need for knowledge management to ensure proactive information and messages to reduce fraudulent online transactions significantly.

The growing technological availability and capabilities of consumers and the susceptibility of the latter to fraud may require banks to address the consequences as an enabled constituent of the volatile 'online-security sphere' spawned by online banking. The main challenge remains to ensure safe online banking to a compromised host of consumers and to address the general ignorance of the measures that exist to prevent interoperability, fraudulent banking transactions and security issues. This study was an attempt to augment the existing body of knowledge on the topic, or, in the words of Mannan and Van Oorschot (2007: 1): "This work is intended to spur a discussion on real-world system security and user responsibilities, in a scenario where everyday users are heavily encouraged to perform critical tasks over the Internet ..."

REFERENCES

Aggelis, V. (2006). Offline Internet banking fraud detection, *Availability, Reliability and Security*. International Conference Proceedings ARES. Retrieved March 29, 2010, from http://ieeeexplore.ieee.org

Andrews, L. & Boyle, M V. (2008). Consumer's accounts of perceived risk online and the influence of communication sources, *Qualitative Market Research: An International Journal*, 11(1):59-75.

Anthonissen. P F. (Ed). (2009). *Crisis communication: Practice PR strategies for reputation management and company survival*. Kogan Page: London.

Barker, R. (2006). The virtual reality of knowledge creation in cyberspace: a knowledge management perspective. *Conference Proceedings, 2nd Biennial Conference of the Academy of World Business, Marketing and Management Development*, 2, (1), 132-142.

—. (2008). Measuring knowledge management in a virtual chat room: a case study, *Communicatio*, 34, (1), 148-172.

—. (2009). A study of knowledge creation and management in virtual communities. *The Journal of Management and World Business Research*, 6, (1), 1-17.

Campbell, D. & Frei, F. (2010). Cost structure, customer profitability and retention implications of self-service distribution channels: evidence from customer behaviour in an online banking channel. *Management Science*, 56, (1), 4-24.

Conway, T., Ward, M., Lewis, G. & Bernhardt, A. (2007). Internet crisis potential: the importance of a strategic approach to marketing communications *Journal of Marketing Communications*, 13, (3), 213-228.

Denzin, N K & Lincoln, Y S. (2003). (Eds), *Strategies of Qualitative Enquiries*. Sage, Thousand Oaks, CA.

DeYoung, R. (2005). The performance of Internet-based business models: evidence from the banking industry. *Journal of Business*, 78, (3), 893-947.

DeYoung, R, Lang, W.W. & Nolte, D.L. (2007). How the Internet affects output and performance at community banks. *Journal of Banking and Finance*, 31, (4), 1033-60.

Drennan, J. Sullivan Mort, G. & Previte, J. 2006. Privacy, risk perception and expert online behaviour: an exploratory study of household end-users, *Journal of Organisational and End User Computing*, 18(1):1-21.

Elliot, D. (2009). The failure of organisational learning from crisis – a matter of life and death, *Journal of Contingencies and Crisis Management*, 17, (3), 157-168.

Evans, M., Wedande, G., Ralston, L. & Van 't Hul, S. (2001). Consumer interaction in the virtual era: some qualitative insights. *Qualitative Market Research: An International Journal*, 4, (3), 150-159.

Fjeld, K. & Molesworth, M. (2006). PR practitioners' experiences of and attitudes towards, the Internet's contribution to external crisis communication. *Corporate Communications: An International Journal*, 11, (4), 391-405.

Gan, C., Clemens, M., Limsombunchai, V. & Weng, A. (2006). A logic analysis of electronic banking in New Zealand. *International Journal of Bank Marketing*, 24, (6), 360-83.

Gonzàlez-Herrero, A. & Smith, S. (2008). Crisis communications management on the web: how Internet-based technologies are changing the way public relations professionals handle business crises. *Journal of Contingencies and Crisis Management*, 16, (3), 143-153.

Greer, C F & Moreland, K D. (2003). United Airlines' and American Airlines' online crisis communication following the September 11 terrorist attacks, *Public Relations Review*, 29(4), 427-441.

Grunig, JE & Grunig, LA. (1992). Models of public relations and communication, in *Excellence in public relations and communication management*, edited by JE Grunig. NJ: Lawrence Erlbaum, 285-325.

—. (2000). Collectivism, collaboration, and societal corporatism as core professional values in public relations, *Journal of Public Relations Research* 12(1), 23-48.

Hasan, I., Zazzara, C. & Ciciretti, R. (2005). Do Internet activities add value? Evidence from the banking industry. Unpublished manuscript, Rensselaer Polytechnic Institute.

Hernando, I. & Nieto, M.J. (2007). Is the Internet delivery channel changing banks' performance? The case of Spanish banks. *Journal of Banking and Finance*, 31, (4), 1083-99.

Lee, E.K., Kwon, K.N. & Schumann, D.W. (2005). Segmenting the non-adopter category in the diffusion of Internet banking. *International Journal of Bank Marketing*, 23, (5), 414-37.

Lin, J.C. & Hsieh, P.L. (2006). The role of technology readiness in consumers' perception and adoption of self-service technologies, *International Journal of Service Industry Management*, 17, (5), 497-517.

Lueg, C. (2001). Information, knowledge and networked minds, *Journal of Knowledge Management*, 5(2):151-160.

Maclaran, P. & Catterall, M. (2002). Researching the social web: marketing information from virtual communities. *Marketing Intelligence & Planning*, 20, (6), 319-326.

MaCliam, J. & Barker, R. (2009). Towards a conceptual model of crises communication with the media in the financial sector: a case study, *Communicare*, 28 (1), 1-23.

Mannan, M. & Van Oorschot, P.C. (2007). *Security and usability: the gap in real-world online banking*. North Conway, NH, USA: NSPW

McMillan, S.J. & Morrison, M. (2006). Coming of age with the Internet: a qualitative exploration of how the Internet has become an integral part of young people's lives, *New Media & Society*, 8, (1), 73-95.

Miles, M. and Huberman, A. 1994. *Qualitative data analysis: an expanded sourcebook*. Sage Publications: Thousand Oaks, CA.

Nonaka, I. and Takeuchi, H. 1995. *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press: New York.

Nusair, K. & Hua, N. (2010). Comparative assessment of structural equation modelling and multiple regression research methodologies: e-commerce context. *Tourism Management*, 31, (3), 314-324.

Polasik, M. & Wisniewski, T.P. (2009). Empirical analysis of Internet banking adoption in Poland. *International Journal of Bank Marketing*, 27, (1), 32-52.

Sathy, M. (1999). Adoption of Internet banking by Australian consumers: An empirical investigation, *International Journal of Bank Marketing*, 17(7), 324-5.

Swart, Y. (2010). *An integrated crisis communication framework for strategic crisis communication with the media: a case study of a financial service provider*. Unpublished Masters degree. Pretoria: UNISA.

Verwey, S, Crystal, A & Bloom, E. (2002). Chaos and crisis: the Swiss bank case study. *Communicatio* 28(2), 28-42.

White, C. (2009). Examining a crisis communication void: the role of context to mitigate issues, *Journal of Communication Management*, 13(2), 176-190.

Zuma, J. (2009). *South Africa's crisis response plan*. Retrieved September 17, 2009, from http://www.southafrica.info