Improving e-commerce security perception in Banking

Fayaaz Moosa Bham

Mini-dissertation submitted in partial fulfilment
for the degree Masters in Business
Administration (MBA)
at
The University of the North-West

Supervisor: Mr. J.C. Coetzee
December 2007

Acknowledgment

This mini dissertation was possible with the support and guidance of many including the respondents of the survey. I take this opportunity to thank all, but wish to mention a few by name for their contribution was invaluable.

- To my family whom motivated and encouraged me; my father (Moosa), my sister (Farzaana), my nephew (Uzair) and niece (Azraa).

- To Mr. Johan Coetzee, my supervisor, for his guidance, direction and encouragement.

- To my friends Sudesh Dajee, Suleman Moola, Muhammed Karani, John Wilson, Zunaid Patel, Zunaid Vanker, Yusuf Vaid, Zarina Bahadur and Shakeel Moola who contributed positively in my endeavours.

- To Dr. Yousuf Ismail Eshak for his support and editing.

Abstract

E-crime has impacted consumer behavioural habits within the banking industry. This affects both the customer and business value, where customers have considered alternatives and the business not realising the return of investment due to diminishing usage.

Combating the illegal activities of perpetrators of crime is seen as a cost to business without any reward. However, proactively acting against e-crime does alter the perception of the channel, returning the trust to customers. However, going beyond the scope and addressing other factors that influence perception provides a competitive edge.

There are at least six factors that influence perception, namely that minds are limited, minds hate confusion, minds constantly evaluate risks (monetary and functional), minds don't adopt to change easily (they prefer a comfort zone), minds are affected by past experience or communication, and minds lose, focus. These are not restricted to the science of consumer behaviour, but need to be considered in both technical decisions and change management.

By influencing the perception of consumers, technology changes and e-commerce threats, which continuously evolve, do not have the same impact. Consumers become aware of their existence and are empowered to deal with the issue at hand.

Probable the greatest influence on perception is knowledge and education. Having a strategy that educates consumers about the operating environment is investing in an organisation's customers lifetime value.

Contents

List of Figures

List of Tables

Chapter 1: Problem Identification and Research Proposal

1.1 Introduction

E-commerce banking has progressed within a relatively short period since the introduction of electronic-based branches in the 1960s, the first ATMs in the late 1970's, the POS (Point of Sale) in the late 1980s and telephone banking, call-centres and Internet banking in the 1990s. The newly introduced mobile solution, with an anticipated but rapid adoption of the technology as mobile phones, with Internet or equivalent features become more pervasive will promote the self-service channel significantly (Cain, 2007:14). Furthermore, the advancement of these self-service channels are extensions rather than substitutes, with the benefits to banking as:

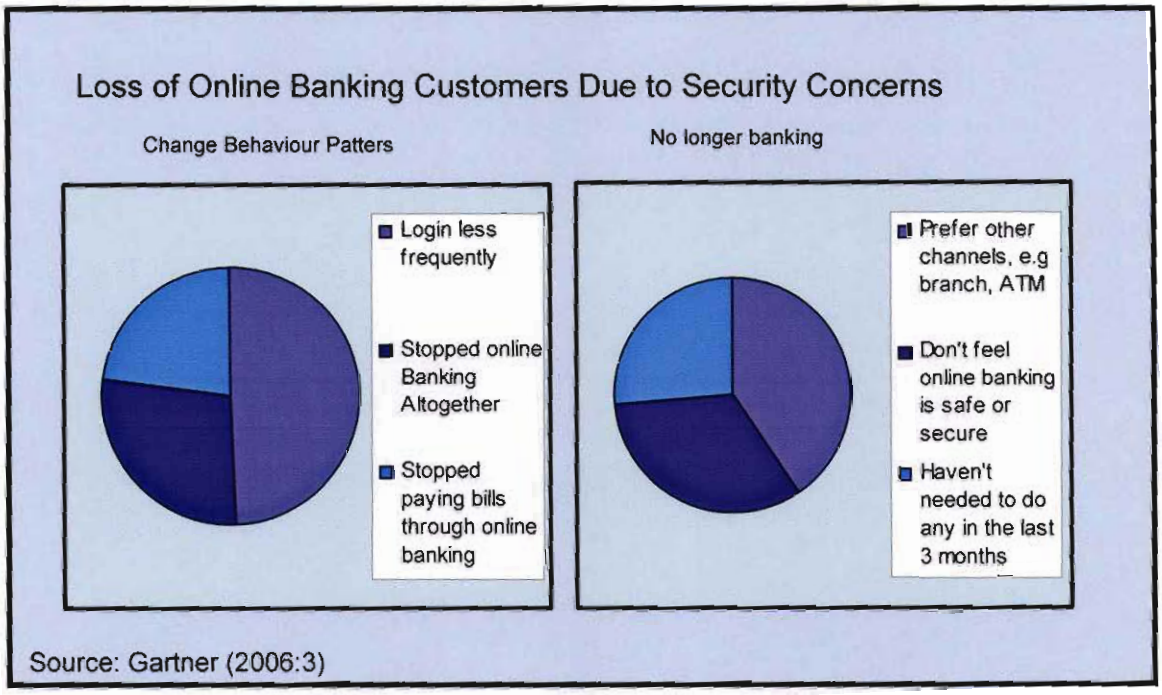
- Availability anywhere, any time,
- Enhancing customer satisfaction
- Improving customer experience
- Improving customer retention

Except for telephone banking, none of these technology-based solutions has had a decaying effect on their predecessor, with anticipated growth in all channels (BMI-T, 2005:23:1). The survey mentions strong short-term growth prospects for Internet banking before reaching its plateau.

However, the Internet-based technologies of Internet banking and mobile banking are at great risk from malice and compromise, as the seemingly endless world of the Internet nurtures and shelters a new generation of hackers, fraudsters and criminals, all champing at the bit to exploit weaknesses within systems for personal gain. Exploiting these weaknesses breaches the confidence

of this type of banking, which adversely affect customer behaviour as indicated below (Gartner, 2006:3):

Figure 1-1: Loss of Online Banking Customers Due to Security Concerns



Successfully exploiting these weaknesses at the expense of customers breeches the trust customers have in the channel. Sklar's (2001:22) opinion is that there is a need to deliver solutions that promote a trusting environment, which is the cornerstone of any e-commerce business relationship. High levels of trust are achieved when importance is given to availability, accuracy, authenticity, confidentiality, integrity, utility and possession. These criteria are the bases of Information Technology Security (Whiteman & Mattord, 2003:10).

White & Nteli (2004:49) identify the quality of service in terms of security levels and trust; and these are amongst others key concerns in the minds of consumers. The bases stems from the results of their survey where traditional banking customers rank security and credibility as the two most important aspects within the ambits of quality of service. Considering the result of attacks

on the Internet platform (figure 1.1), it becomes natural to focus on the impact it has on the growth and adoption rates of Internet and mobile banking.

Any negative impact of usage and growth affects the expected financial returns of the channel. In this scenario, the loss of trust and credibility impacts usage of the channel negatively, adversely affecting the customer lifetime value (CLV), which reflects on any organisation's profits. Furthermore, Stenzel, Cokins, Flemming, Hill, Hugos, Niven, Schubert & Stratton, (2007:228) mentions the cost of acquiring new customers as being greater than retaining existing ones.

Considering the potential negative impact of trust and credibility within the e-commerce space, the goodwill of a customer is paramount. This provides the bases of the study. Banks need to address issues that challenge the sanctity of trust and credibility and they need to promote a favourable and reassuring campaign that improves the perception of the customer.

"Perception is reality. Don't get confused by facts" - (Trout, 2004:34).

1.2 Background

Over the last decade, the rapid evolution of the self-service banking channels, namely point of sales (POS), automated teller machines (ATM) and the virtual channel of Internet banking, has drastically changed client experience of banking. These rapidly evolving channels have broken down the traditional "brick and mortar" barriers to banking thereby extending banking 24 hours a day, across national and international borders and at conveniently located access points. The effectiveness of these remote facilities is reflected in the unprecedented growth of the channels supported by an ever-changing technology landscape.

The traditional form of banking; book-based with an authentication means of physical presence, signature comparison and visual identification has been transposed to a card / profile based instrument, which activates the banking facility with an authentication token, e.g. a PIN. This shift of security changed from one of physical to that of virtual, whose assurance rests within the realm of information technology security.

Information technology security has been influenced largely on two fronts over the years

- The scope of information security keeps on expanding
- The ultimate responsibility for information security has moved over the years (Von Solms, 1996:281)

Today, ten years hence, the inclination remains, with security controls being integrated with technology changes and boundaries of responsibilities expanding beyond the organisation's structure.

The channels that constitute the self-service banking offering can be segmented into two streams, based on the characteristics use and governance (Arunachalam & Sivasubramanian, 2007:1). ATM and POS involves the use of a card (magnetic stripe or chip card) and a known authentication token, in the form of a personal identification number (PIN), operating within a controlled and institution-owned environment. This controlled environment is governed by common card associations, namely VISA, MasterCard, Europay and Bankserv (Saswitch). In contrast, the Internet banking channel is institution specific, does not operate within an association controlled network and uses either a card or profile as an access method with multiple forms of authentications.

Both streams are affected by fraud. Whereas the former is regulated by defined rules, the most prominent being that defined in the Payment Card Industry (PCI) Data Security Standard (PCI Security Standards Council, 2006:2), the latter, i.e. Internet banking is dealt with by individual banks. The Standard ensure a high

level of security by defining twelve requirements which all members, merchants, service providers and third party processing vendors need to adhere to.

Referring to the aforementioned impact of security (figure 1.1) it is evident that IT Security cannot be a reactionary measure alone. It has become the responsibility of the banks to implement pro-active solutions to protect customers' interest, thereby not having to rely on incidents to promote the need for security which is supported by Litan (2006a:2). He recommends fraud detection methods within authentication services to complement online banking.

Furthermore, the change in behavioural patterns as evident in figure 1.1 can be counteracted by a perception-altering strategy, which focuses on the factors that influence perception. These factors are: minds are limited, minds hate confusion, minds constantly evaluate risks, minds do not adopt change easily, minds are affected by past experiences and minds lose focus (Trout, 2004:13-34).

1.3 Problem Statement

The continual attacks on Internet banking create a negative sentiment:

- Users are becoming weary and doubt the channel's integrity to be a relatively risk free means of transacting;
- The supposed benefits of using the channel at any location, be it a public access point (such as an Internet Café) or wireless establishment environment, is discouraged by the financial institutions;
- The lucrative illegal trade is growing at an alarming rate with more compromises reported and more people being targeted;
- The warning of fraud that is communicated in the press creates panic rather than awareness.

The result is a negative perception of the e-commerce solution, i.e. Internet banking, which undermines the growth and usage of this banking platform.

Furthermore, the feeling may be passing on to the mobile banking technology as it is based on the Internet platform.

The problems identified for this study, which stems from the change in customer behavioural patters and Internet Banking attrition as depicted in figure 1.1 are:

- A significant number of Internet banking users have a perception that the security provided by the Internet banking solution is inadequate for their satisfaction.
- Information security attacks and concerns negatively affect the confidence of Internet banking

1.4 Objectives

The study is to investigate various concepts that explain the interaction of business, customers, processes and technology that will help address the problem which leads to the objectives.

1.4.1 Primary Object

The primary objective of the study is to address the stated problem as follows:

- Determining if the factors that influence perception have an effect on confidence in the Internet and mobile channel
- Determining the relationship of *Confidence* to *Perception* and *Quality of Service*

1.4.2 Secondary

The secondary objectives are

- A Strategy to influence security perception by addressing e-commerce security matters
- A change management strategy for the implementation of security solutions and features that minimise impact on clients

- A proposed fraud management-solution based on individual behavioural habits to reduce financial risk to customer and bank

1.5 Constraints

The study is limited to banking in South Africa as rules and regulations vary from country to country. Furthermore, the study covers traditional retail banking and excludes business, specialised or private banking, as these types of banking follow a focus or strategy where the interaction with the target market is concentrated, specific or restricted.

The study is restricted to the middle and upper-middle economic segment as they constitute the majority of Internet banking users. The lower segment is excluded as they predominantly use the ATM and POS channel to fulfil their needs, which are cash dependent.

Furthermore, e-commerce banking has diverged into two streams as mentioned above, the ATM/POS segment and the Internet-Based segment, which includes mobile based banking. The study excludes the ATM/POS segment as it is association-controlled and regulated, but references it.

The literature has been sourced from published books, articles, and news reports, post 1998, and is readily available from South African libraries. The remainder is available from subscriber institutions, the Internet, and the public domain.

1.6 Methodology and layout

The argument of this research is presented as follows:

1.6.1 Literature Study

This section presents the related disciplines of business management that explain and/or influence the objective of the research i.e. provide arguments pertaining to the adoption and usage rates of the Internet banking and mobile banking channels. It provides the foundation of the empirical study, depth within the analysis phase and helps to substantiate arguments in the recommendation and conclusion. The disciplines covered are:

- Technology and Information Technology management
- Information Security management, inclusive of risk management
- Consumer Behaviour in particular the perception of customers
- Change Management

1.6.2 Empirical Study

The empirical study tests the validity of the problem statement which will determine the direction of the recommendation. The empirical study includes the collection of data from a survey completed by a random sample of users residing within the Johannesburg areas, South Africa. The interpretation and analysis of the data concludes the empirical study, using statistical techniques based on Field's Discovering Statistics Using SPSS (2005) and Wisniewski's Quantitative methods for decision makers (2002).

1.6.3 Result Analysis

The result analysis section places the Internet banking channel into context of the presented literature and applies the findings of the survey. This enables the drawing up of concise recommendations which conclude the study.

1.6.4 Recommendations and Conclusion

This section recommends the solution to the problem statement and concludes the study.

1.7 Chapter Layout

The layout of the research study is as follows

- Chapter 1 - Problem Identification and Research Proposal
- Chapter 2 – Literature Study
- Chapter 3 – Empirical Study
- Chapter 4 – Result Analysis, Recommendation and Conclusion

1.8 Summary

The escalation of attacks on online banking has disrupted the Internet banking channel, to the extent that banks have to take an aggressive stance to avoid loss in customer value. The resultant impact is a negative perception of the channel, undermining the confidence of Internet banking users. Hence Banks need to be more pro-active and implement counter-strategies to mitigate the risk of these threats.

The aim of the study is to address the problem by understanding the customer, the relationship of customer perception to confidence and dealing with the problem based on customer feedback.

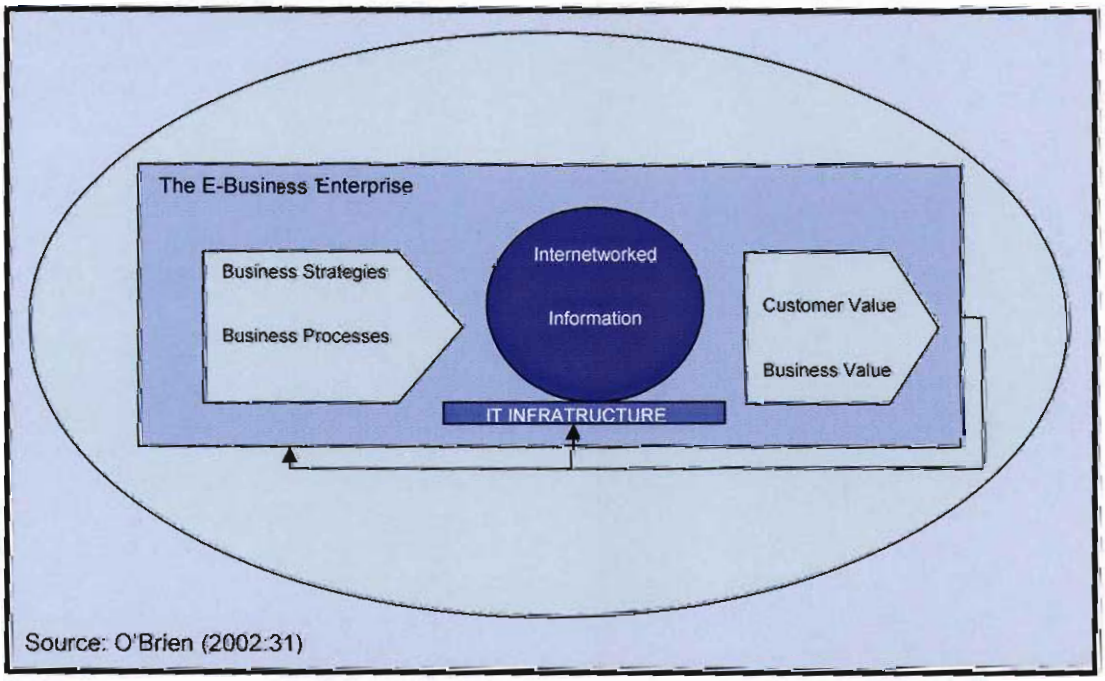
Chapter 2: Literature Study

2.1 Introduction

An information system is a combination of people, hardware, software, communication networks and data resources that is processed into meaningful information (O'Brien, 2002:7). When combined with supporting technologies and efficient information management practices, an e-commerce solution is achieved. The e-commerce solution's objective is to support business strategies, business processes and organisational cultural structures to increase customer and business value as depicted in Figure 2.1.

The model indicates a cyclic relationship between customer and business values and IT infrastructure that fulfils an organisation's strategic and processing objectives. The state of the IT infrastructure, which is reliant on supporting technologies, will determine the effectiveness of an e-commerce solution.

Figure 2-1: E-Business Enterprise Model



The change in customer behaviour as depicted in figure 1.1 directs the primary objective of the study; to determine the factors that influence perception, in particular those relating to e-commerce security. This will enable the secondary objective to recommend improvements that will extract customer and business value.

Of the ten competitive forces, i.e.

- Supplier bargaining power
- Customer bargaining power
- Threat of substitute services
- Rivalry amongst existing firms
- Threat of new entrance
- Digitisation
- Globalisation
- Deregulation
- Transparency
- Institutionalised competitive forces (van Buuren, 2006:36)

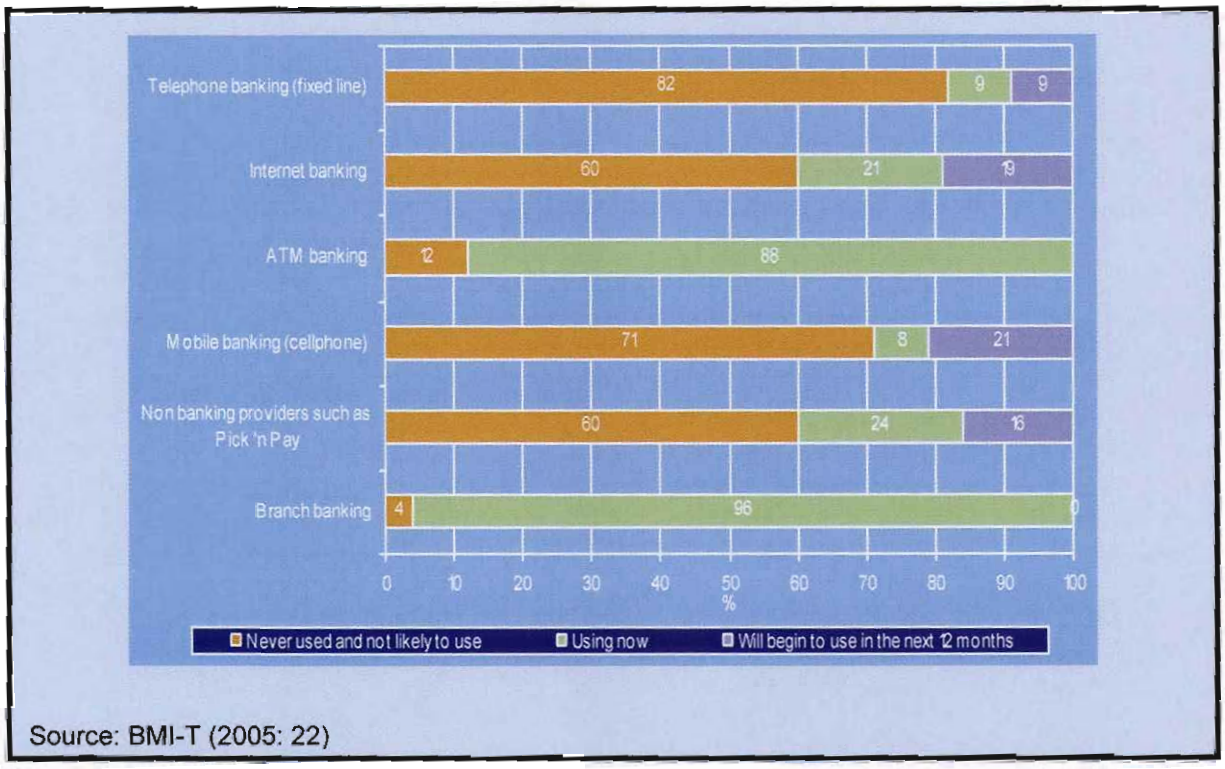
customer bargaining power and digitisation are significant to the study and will be presented in an applicable context referencing of technology management, information security management, e-commerce management, cyber-law and consumer behaviour. This literature study is completed by referencing appropriated aspects of risk and change management.

2.2 E-Commerce within Technology Management

2.2.1 E-commerce Adoption Life Cycle

Self-service banking comprises of a number of technology-based solutions, which are segmented into two dominant streams, namely the ATM/POS channel and the Internet/mobile banking channel. These two streams' current and future adoption and usage are significantly different as depicted in figure 2.2.

Figure 2-2: The Changing Face of Banking in South Africa

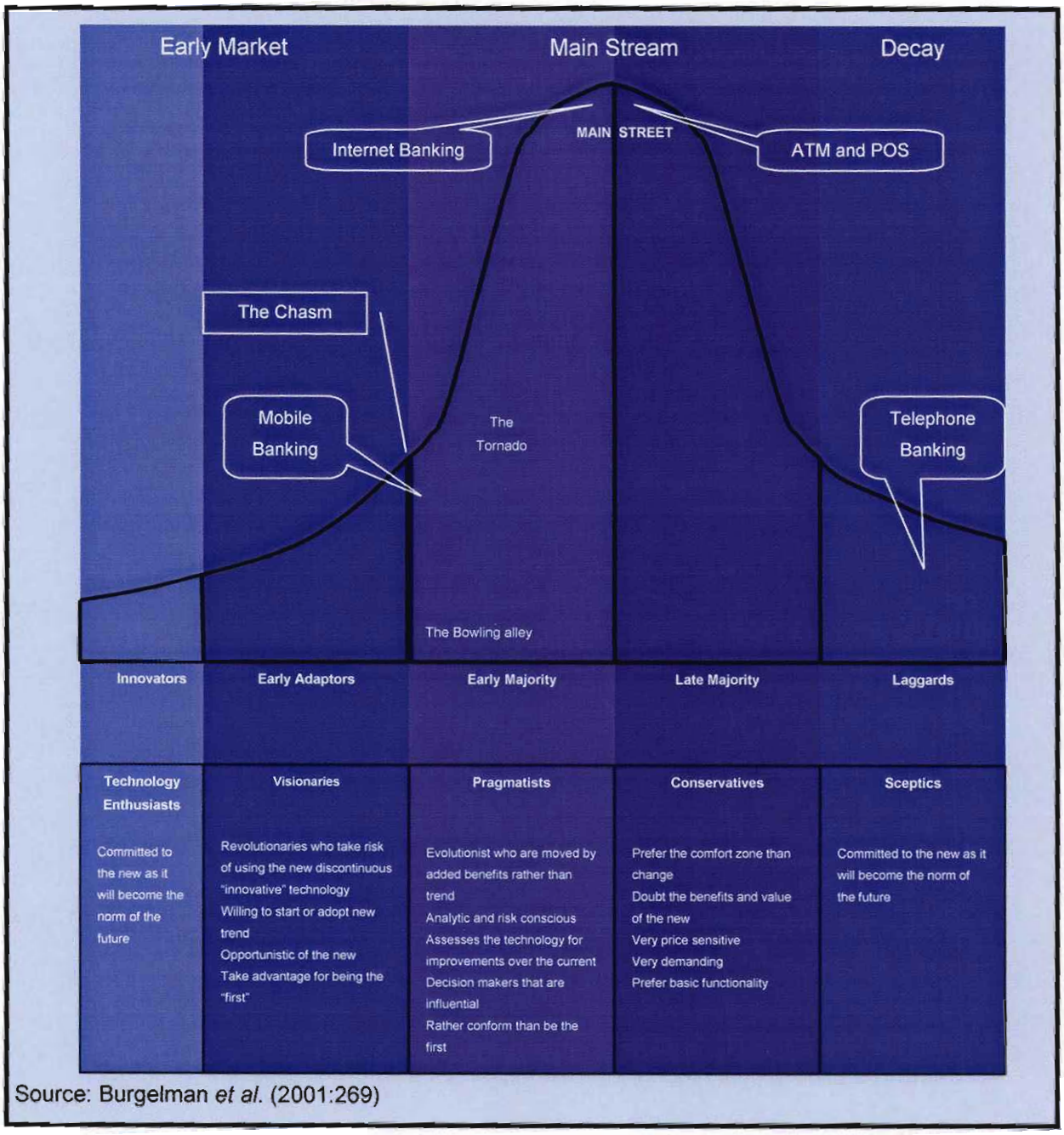


Source: BMI-T (2005: 22)

These technologies were discontinuous innovations when introduced into the market, which radically affected the market by changing customers' behaviour from a customary one to new way. The convincing factor that enable the change was the premise of attaining equal or better benefits to that of the old (Burgelman, Maidique & Wheelwright, 2001:266).

However, consumer behaviour varies, creating market segments based on personalities as depicted by the technology adoption life cycle model below. The traits and characteristics of consumers are tabled within the model.

Figure 2-3: The Technology Adoption Life Cycle



Source: Burgelman *et al.* (2001:269)

Burgelman *et al.* (2001:268) identified inflection points as indicated in figure 2.3 as follows:

The chasm - a critical point in a technologies life cycle: The key to crossing the chasm is convincing the pragmatist that the innovation has benefits and providing proof that success and not failure will be the outcome, i.e. the innovation is within an acceptable risk to adapt to realise better benefits.

The bowling alley – niche-based promotion: Where the product is glossed for a focused but niche market prior to general adoption. The aim is to use a niche-based strategy that is customer-centric with the ultimate aim of gaining a favourable position that will be used to convince the early adopters.

The Tornado – when the technology is adopted in masses: This occurs when early adopters commit to the technology driving the strategy to cater for a mass-market. Such strategies involved standardising the technology.

The Main Street – the technology has matured: This stage can be identified when adoption rates plateau, warranting the need for aftermarket add-ons to prolong the plateau. To effect this, the strategy reverts to customer-centricity, focusing on value adds.

End of Life – the demise of the technologies. Occurs when substitutes or innovations rapidly erode the use of the current technology until demise.

Positioning the technology within the life-cycle allows one to implement the appropriate strategy to ensure a sustained growth. The information contained in the channel usage graph (figure 2.2 above) places the self service channels as follows:

- ATM & POS - Late Majority (88 % adopted)
- Internet banking – Early Majority (21 % adopted and 19 % will adopt to, and 60 % will never use).
- Telephone Banking - End of Life (82 % will never use, 9 % adopted, 9 % will adopt)
- Mobile banking – crossing the chasm (8% adopted, 21% will adopt and 71% will never adopt)

Based on the position within the technology life cycle, the appropriate strategy is tabled below using the aforementioned arguments of Burgelman *et al.* (2001:268).

Table 2-1: Adoption Characteristic / Strategy Matrix

Channel	Characteristic	Dominant Users and	Strategy
ATM / POS Banking	• Extremely popular especially for cash withdrawals • Usage will not decrease	Late Majority / Conservatives	In the Main Street – requires a customer-centric approach.
Internet banking	• Growth at the expense of branch banking. • Usage will increase but plateau	Early Majority / Pragmatist, however appealing to the Conservative	Approaching the Main-Street. Shift from Standardisation to customer – centric
Mobile banking	• Opinion is that that adoption will not be Readily accepted by average users • Slow growth in uptake • Appeals to a select market – niche	Early Adopter / Visionaries	Niche and focus Strategy
Telephone banking	• Process of attrition • Usage decreasing • Low levels of new users	Laggards/Sceptics	Planned for exit – Strategy is to migrate users to Internet or mobile banking. Alternatively look for options within the Call Centre / Speech banking offering.

Evident from the Adoption model (figure 2.3) is the position of the technology, which determines the strategic action needed:

Internet banking: - Focus on the customer and the provisioning for value-added features. The mitigating actions to e-commerce attacks can be packaged as a value-add feature.
Mobile banking: - A focus strategy that is niche, intended at a limited but influential market that will be the catalyst for growth. Once growth is achieved, the strategy changes to standardisation.

Any strategic change to a technology incurs costs, which need to be justified as viable. The future value of benefits materialised from cost can be mapped.

2.2.2 The E-Commerce Customer Lifetime Value

Stenzel *et al.* (2007:252) calculates the Customer Lifetime Value (CLV) using ten variables namely,

1 - Acquisition and upgrade costs [- to value],
2 - Recurring revenues [+ value],
3 - Recurring cost to serve customers [- to value],
4 - Up and cross selling [+ to value],
5 - Credit and returns [- to value],
6 - Renewal and retention promotions [- to value],
7 - Downward migration [- to value],
8 - Bad debt and removal cost [- to value],
9 - Churn and attrition [- to value] and
10 - Win-back [- to value].

As the customer lifetime value bears directly onto an organisation's profit, efforts are needed to minimise cost and maximise revenues.

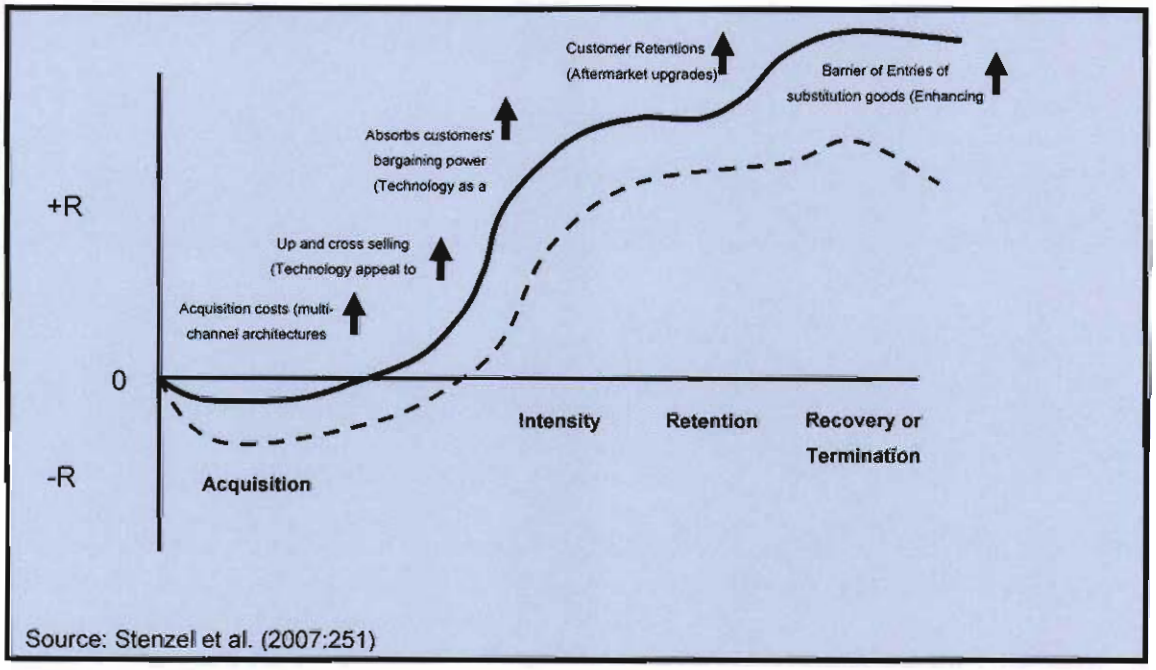
Technology related costs that affect the CLV (fully or partially) directly, such as acquisition and upgrades of systems and recurring costs to serve customers (maintenance of Information systems) can be contained by using a multi-channel architecture. The business and customer values are reaped when multiple

technology solution use common processing platforms on a comprehensive architecture with the only difference in the end-presentation of the solution to customers (Macknight, 2005:12).

Furthermore, technology innovations and upgrades can prevent downward migration by aiding in customer retentions, support up and cross selling, repelling forces of substitution services and absorbing customers' bargaining power (Stenzel *et al.* 2007, 228-230). The net effect of these initiatives is illustrated in figure 2-4.

Without the use of multi-channel architecture, the net acquiring cost is higher, causing the CLV curve to be lower as indicated by the dotted line. Technology that succeeds through the chasm with relative ease will have a higher CLV. Similarly aftermarket upgrades drives the CLV upwards by supporting customer retention initiatives, absorbing customer bargaining power and protecting against the digitalisation threat of cyber crime.

Figure 2-4: Customer Lifetime Value



Source: Stenzel et al. (2007:251)

Introducing new technologies to gain business and customer value changes the landscape of the e-commerce environment and opens up new possibilities.

2.3 *Impact of Supporting Technologies on E-Commerce*

The information technology landscape transforms at an unprecedented pace when compared to any of the previous ages such as the industrial age, the cold war, etc. Industry leaders have modelled the phenomena as follows:

Moore's Law - "Processing Power doubles every 18 months"
Glider's Law - "communication bandwidth doubles every 6 months"
Metcalfe's – "the community value of a network grows as the square of the number of its users increase. "
Less's Law - The cost of storage is reduced to half every 12 months, while capacity doubles within the period.

These laws explain the role of supporting technologies of hardware processing power, storage capacity and networking on the rapid growth of information processing. Metcalfe's law is generally cited as an explanation to the continuous boom in the number of Internet users, Moore's the downward costs of hardware, and Gilder's in the advancement and added features of Web applications (Simon & Shuster, 2001), (Shibayama, 2007) & (Intel, 2007). The result is a rapidly changing landscape with growth in new users, and the expansion of Internet capabilities. The impact on e-commerce is positive to processing and development but tends to be negative in that it empowers criminals in illegal activities.

2.4 *E-Commerce within Information Technology Security*

Schneider (2007:5) quotes the IBM definition of electronic business (e-commerce) as "the transformation of key business processes through the use of Internet technologies". He presents his works with dedicated emphasis to the environment of electronic commerce (legal, ethical and tax issues) and electronic commerce security.

2.4.1 Electronic Commerce Environment: Legal and Ethical Issues

Laws, regulations and accords that define the legal and regulatory banking landscape are strictly enforced by the South African Reserve Bank and include amongst other the following:

Bank Act (94/1990): The base act with which any institution that wishes to trade as a bank must comply. It is the general act which defines the rules for banking

Financial Intelligence Centre Act (38/2001): The act to combat money laundering activities

Electronic Communications Act (36/2005): The objective of this act is to define the legal requirements of electronic communications and transactions within the public domain, inclusive of the Internet.

Basel II Accord- Is a comprehensive framework which sets and measures regulatory capital adequacy requirements that are aligned to the underlying risk a bank faces (present and future). This revised accord is more flexible and adaptable to changing market conditions, thereby allowing better risk management practices (Basel Committee on Banking Supervision, 2005:7).

King II – The King Report on Corporate Governance defines both the responsibility and accountability onto directors of organisations, at board level, such that they become answerable on governance and performance

issues and general affairs that affect stakeholders. The ultimate responsibility remains at board level, negating the possibility of being absolved due to delegation (Institute of Directors in Southern Africa, 2002: 10-12).

Association Compliancy – All banks in South Africa must subscribe to the Payment Association of South Africa (PASA), as stipulated in the Bank Act (94/1990). The association has extended the legal requirement to allow inter-operability. Furthermore, most of the major banks belong to at least one of the international associations, namely MasterCard, Visa, Diners Club, American Express or Europay. MasterCard and Visa have mandated members to comply with the Payment Card Industry standard which is discussed later (PCI Security Standards Council, 2006:2).

However, two factors of e-commerce are identified by Schneider (2007:311) that create difficulties in the legal framework, namely:

- The Internet traverses countries physical boundaries, where they may be subject to additional laws or our laws may not applicable.
- The Internet community has very high levels of interaction with other businesses and users. The cumulative effect of the Internet community has significant "buying power" that can negatively affect e-commerce businesses if they are perceived to be unethical or unfair.

Ethics are closely coupled to cultures which were previously restricted within geographic boundaries. The Internet dismantles these geographic boundaries, forcing organisation leaders to adopt an extended set of ethics in addition to the one prevailing within the physical location of the organisation. Schneider (2007:335) mentions the importance of considering global ethical issues in policy and procedural decision-making.

The concerns regarding legal deficiencies that arose from the popularisation of Internet have forced many governments to introduce legislation to control electronic communications. Within the South African context, the Electronic Communications Act (36/2005) was gazetted in 2005 to regulate the Internet industry more effectively.

2.4.2 Electronic Communications Act: Implications on E-Commerce

The Electronic Commerce Act (36/2005) does not define "electronic-transactions" as a specific entity, but defines transactions as either commercial or non-commercial, including a *provision for information* and e-government services (Buys, 2004:141). The "provision for information" implies that as soon as a customer enters a web site, he has entered into an "electronic transaction" thereby being bound by the terms of the Electronic Communications Act (36/2005).

The act covers a broad spectrum of entities relating to the mechanisms of e-commerce such as

- Legal requirements for data messages,
- Communications of data messages,
- Retention of messages,
- Doing business online,
- Contract requirements,
- Offer and acceptance,
- Cryptography, certification and electronic signature,
- Consumer protection,
- Privacy.

2.4.3 Card Association Intervention on E-commerce

Over the years, the various card associations enforced a strict code of conduct to franchisees, in order to protect the integrity of their transacting solution. In 2004, the two dominant associations, namely Visa and MasterCard, introduced the

Payment Card Industry (PCI) Data Security Standard which defined the requirements to secure a transacting network. All franchisees were mandated to comply with the standard, and any failure to comply will resulted in a liability shift of fraud to acquiring institution and the risk of having their licence revoked (PCI Security Standards Council,2006:2).

The PCI Data Security Standard covers the implementation of the six pillars of Information security as mentioned by Schneider (2007:443) namely:

- Secrecy (confidentiality) – usable data and readable information is available only to those it is intended for,
- Integrity – data and information will remain as it is intended to during the course of its life span without any alterations ,
- Availability – that data, information and processing system will be fully operational to accomplish its object as per requirements,
- Key Management – that encryption keys used will be managed accordingly,
- Non-repudiation – that sufficient logs and control are in place if an event has occurred and disclaim "denial" ,
- Authentication – the access to systems and resources are validated against know credentials.

And the additional

- Authorisation – that access to systems and resources is within the defined scope

The standard details the implementation of security controls under the categories of securing networks, protecting cardholder data, maintaining a vulnerability management programme, implementing strong access control measures, regularly monitoring and testing networks and maintaining an information security policy.

The 12 auditable requirements that cover the aforementioned categories are:-

- Firewall management
- The use of default passwords and security parameters
- Storage of cardholder data
- Encryption of data in transit
- Use of the latest anti-virus software
- Developing and maintaining secure systems and applications
- Restriction of cardholder data to those that need it
- Non-sharing of user-IDs and accounts
- Restriction of physical access of card holder data
- Tracking and monitoring of all access to network resources and cardholder data
- Validating security systems and processes regularly
- Maintaining an Information Security Policy that is reviewed regularly

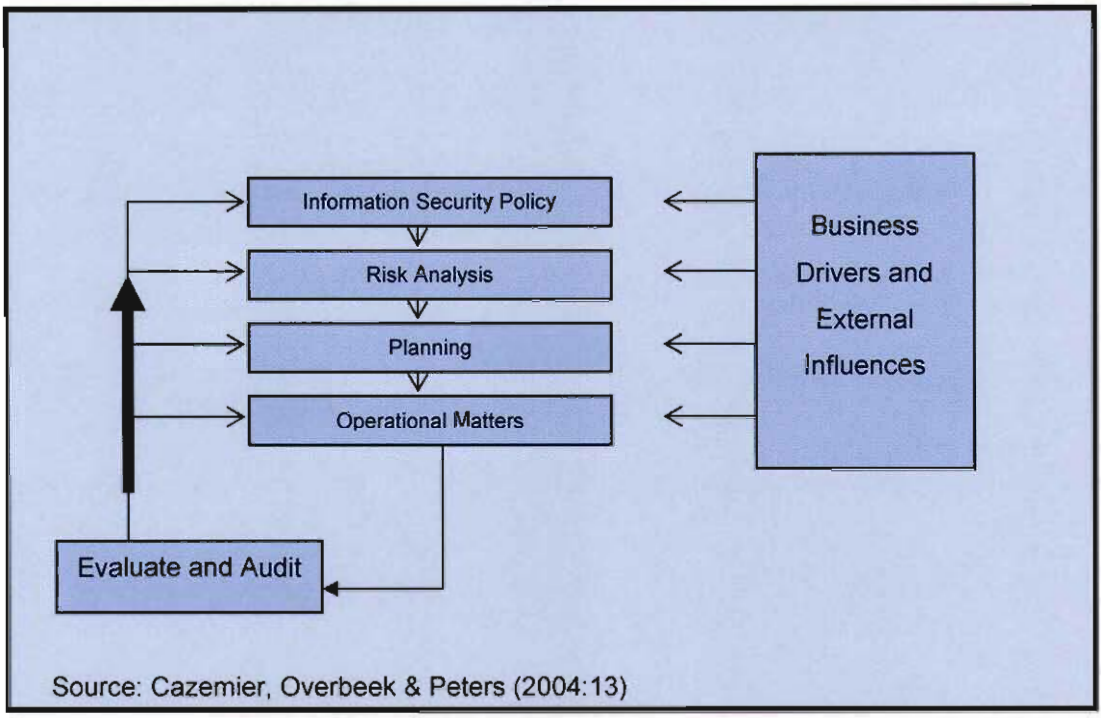
Considering the requirement of King II, i.e. the need of good corporate governance and the Basel II accord that stipulates the capital adequacy to cover the underlying risk, these requirements will be met by most organisations using an appropriate model.

2.4.4 Information Security Model

Schneider (2007:442) stresses the importance of an organisation having a security policy in place that protects electronic information which is one of the most valuable assets of any organisation. He mentions that a sound security policy contains the assets to be protected, the reason for the protection, the persons responsible for the protection and the allowed actions on the information asset.

To facilitate the policy, risks are continuously evaluated and appropriate controls formulated to mitigate the risk. These risks emanate due to business drivers or external influences (inclusive of threats) that affect policy, planning and operations matters as depicted in figure 2-5.

Figure 2-5: Security Framework Model



The intent of a security model method is to provide a framework for self-inspection that binds policy, risks, threats and controls. Organisations that prosper often reflect on their own situation guarding against the ten deadly sins of information security (von Solms & von Solms , 2004:372):

- Not realising that information security is a corporate governance responsibility
- Not realising that information security is a business issue and not a technical issue
- Not realising the fact that information security governance is a multi-dimensional discipline
- Not realising that an information security plan must be based on identified risks
- Not realising the important role of international best practice for information security management

- Not realising that corporate information security policy is absolutely essential
- Not realising that information security compliance enforcement and monitoring is absolutely essential
- Not realising that a proper information governance structure is absolutely essential
- Not realising the core importance of information security awareness amongst users
- Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities.

Having a sound information security strategy that is implemented effectively alleviates the burden of risk management.

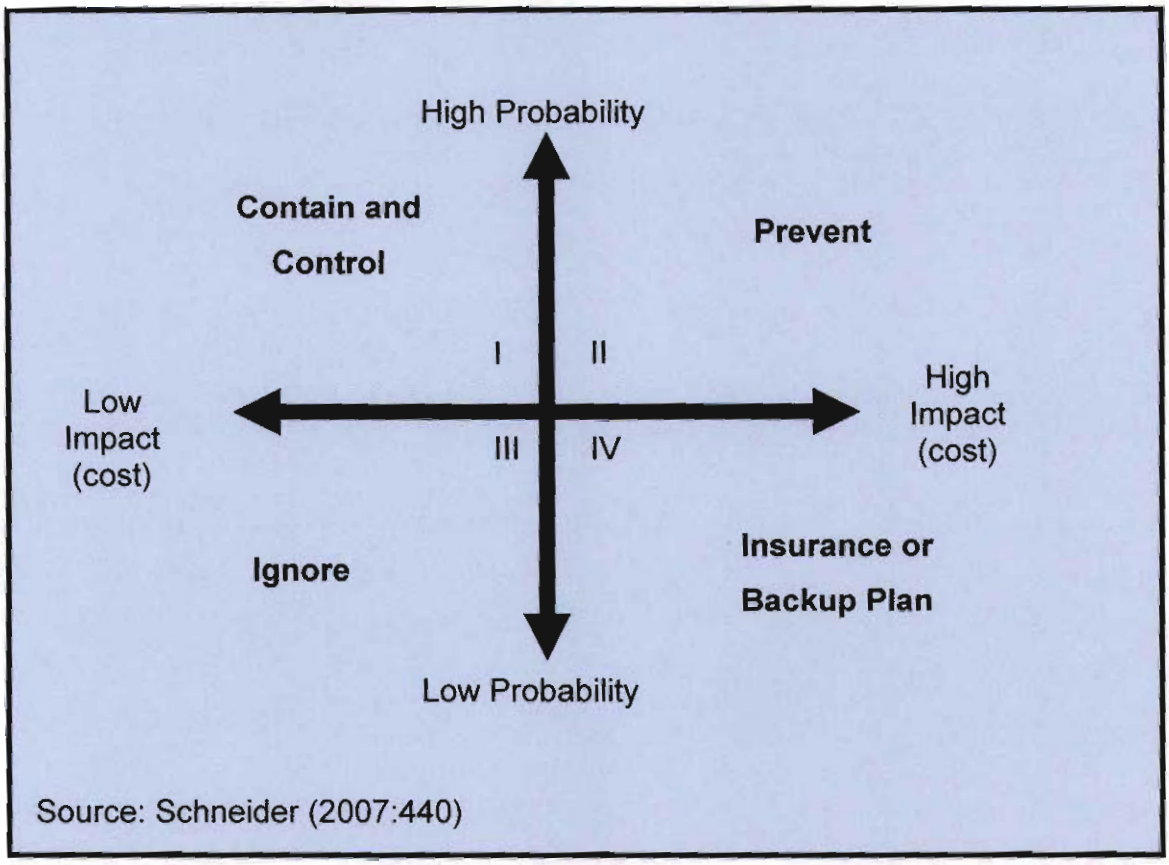
2.5 Risk Management

2.5.1 E-Commerce Risk Management Model

Schneider (2007:440) presents a basic risk management model that determines the extent of a counter-measure that is required to mitigate the effects of a threat.

The security model presented evaluates risks on the probability of occurrence and the impact if the event materialises. Von Solms (2003:3) mentions that it is common practice to categorise these risk on a high level into technical, logical, human, physical and environmental which helps but does not ensure effective management. He suggests using an industry model such as COBIT (control objectives for information and related technologies) that defines 34 IT governance processes that require attention.

Figure 2-6: Risk Management Model.



The challenge of computing the value of the impact of a threat within the information technology space (Steward, 2004:363) is that the event cannot be measure against historic data, whereas other events such as a house fire or burglary in an area can be measured based on the past. Furthermore, the growth of the Internet means a greater exposure to criminal syndicates which grow at least at the same rate of the Internet. Hence risks cannot be measured but compared to the industry. Likewise the effectiveness of the controls are reflected in the position an organisation finds itself, when compared to its peers within the same industry. Nevertheless, the expected cost of the impact given the chance of it happening will determine the action needed as depicted in figure 2-6.

2.5.2 E-Commerce Threats

Schneider (2007:444-487) discusses a number of threats, such as denial of services attacks, propagation of virus and Trojans, application defects and exploitation of operating system vulnerabilities, all of which contribute to the negative sentiment of Internet banking. All these attacks are controlled and mitigated within the Security Framework and Risk Management models (Figure 2-5 and figure 2-6, respectively). However the indirect Internet threat of Phishing, which doubled between 2004 and 2006 (Litan, 2006b:1), requires intervention that includes the customer.

Phishing is a concept of using the Internet platform to perform a social-engineered attack. A social-engineered attack is an attack that deceives one into doing an action which he or she would not have ordinarily have done for a stranger (Mitnick, 2002:xi). The success of such an attack within the technology realm is attributed to the power of applications to "mimic" the attack as a genuine approach by an organisation to obtain user's sensitive details for "some form of confirmation". Typically the sensitive details requested are user-names passwords, credentials, demographic information, etc that can be used later to complete an identity theft (Mitnick, 2002:175-180). Sensitive details are then used to access the user Internet account or used to obtain other credentials or items to complete the operation.

The shift of Internet attacks from organisations to their customers extends the problem into a broader domain that affects customer behaviour. An understanding of the impact will help organisations deal with the problem more effectively.

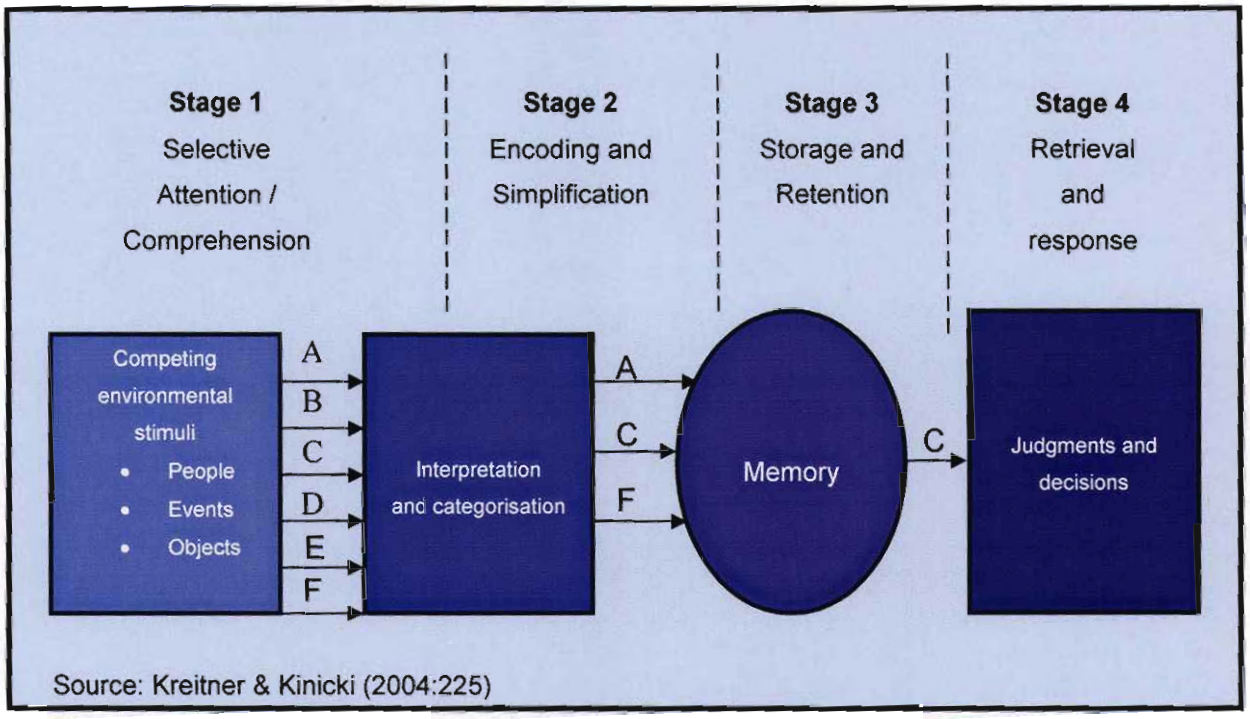
2.6 *Consumer Behaviour*

2.6.1 Understanding Perception

The definition of perception is described as "the process by which an individual selects, organises, and interprets stimuli into a meaningful and coherent picture of the world" (Schiffman & Kanuk, 2004: 158). According to this definition, we can assume that people ultimately develop a subjective viewpoint of the world around them based on the information that they receive or the experiences that they have had. This would then determine their response to events, products and/ or services offered.

Kreitner & Kinicki (2004:225) portrays perception in an information-processing model with defined stages that filters, stores, retrieves and translates information into future actions as depicted in figure 2-7. The filtering stage (stage 1) blocks information that seems inappropriate (or of low impact to the individual), the second maps the information into simplification, the third store the information and the fourth uses the stored information to make a decision of judgment.

Figure 2-7: An Information-Processing Model



Elaborating further, people tend to build their perceptions on the "physical stimuli" presented to them from external environments and their own experiences (Schiffman & Kanuk, 2004:168). Their own experiences, motives, learning patterns and expectations that they have developed previously contribute significantly to the view of the subject.

People reject and accept ideals and information that they view as specially relevant to them and which falls in line with that which they view as applicable (Schiffman & Kanuk, 2004: 172). They do this by "actively" choosing the messages that they wish to be exposed to (i.e. selective exposure) and the attention that they give to the messages or stimuli i.e. selective attention. They may choose to, for instance, ignore all marketing messages of Internet banking all together or only expose themselves to rely on "stimuli" regarding Internet banking if they have a nature that take risks.

In addition to the above two issues of selective attention and selective exposure, consumers rely on perceptual defence and perceptual blocking. Perceptual defence refers to the clients' ability to screen out issues or messages that are "psychologically threatening'. This is a subconscious act (Schiffman & Kanuk, 2004: 172). Perceptual blocking is when the consumer consciously "tunes out" from receiving the stimuli (Schiffman & Kanuk, 2004:172).

Perception development is based on the individual's reaction to the stimuli received. He or she chooses to accept certain stimuli while rejecting others (Schiffman & Kanuk, 2004: 168). An individual's expectations are influenced by their past experience or a general understanding of what is expected (Schiffman & Kanuk, 2004: 169). The client will therefore accept certain ideas while rejecting others based on previous experience.

2.6.2 Impact of E-commerce events on Perception

The industry is sensitive to e-commerce threats as indicated in figure 1-1. The change in customer behaviour is attributed to the perception that Internet banking is not entirely safe and as such has created hesitancy in the use these services, irrespective of any other benefits that may arise. In this scenario a lack of trust develops, which compromises an element of quality of services – trustworthiness.

The definition of learning is described as "changes in an individual's behaviour arising from experience". The "lessons" learnt by these individuals determine their perception of the service. Perception and hence their behaviour will be influenced by people's beliefs and attitudes. Beliefs are "a descriptive thought that a person holds about something", whereas an attitude is "A person's consistently favourable or unfavourable evaluations, feelings, and tendencies toward an object or idea". People learn from their experiences and the actions that they have taken. Based on these definitions of beliefs and attitude, it is

imperative that banks actively address negative perception to avoid the perception turning into belief (Kotler & Armstrong, 2004:168-196). To change a belief requires much more effort that to change attitude.

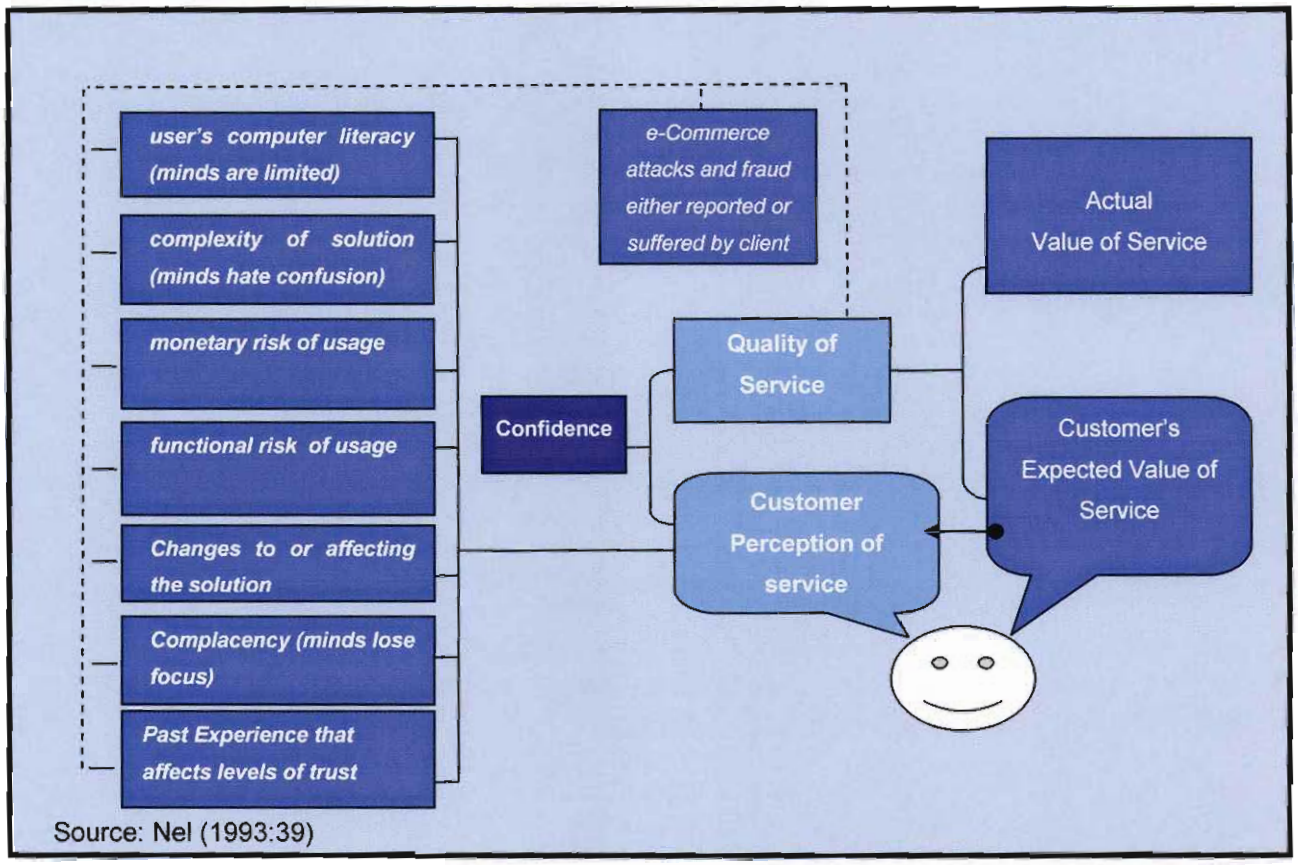
2.6.3 Influencing Perception

Trout (2004:13-34) presents a "changing perception" strategy to improve the position of an organisation within an identified market, which comprises of a collection of individuals. He examines the state of the mind and counteracts the negatives to change the mind-sets. Factors influencing mind-set are:

- Minds are limited;
- Minds hate confusion;
- Minds constantly evaluate risks (Monetary and Functional);
- Minds don't adopt change easily (they prefer a comfort zone);
- Minds are affected by past experience or communication; and
- Minds lose focus.

Using a perception strategy to mitigate the negative sentiments of cyber crime (figure 1-1), the organisation can effectively reposition the channel giving consideration to the mind-set of the customer. Applying the aforementioned factors of perception to the Service Quality Gaps Model [after PZB 1985] of Nel (1993:38) an adapted model is conceived as follows:

Figure 2-8: Confidence, Perception and Quality of Service Model



Source: Nel (1993:39)

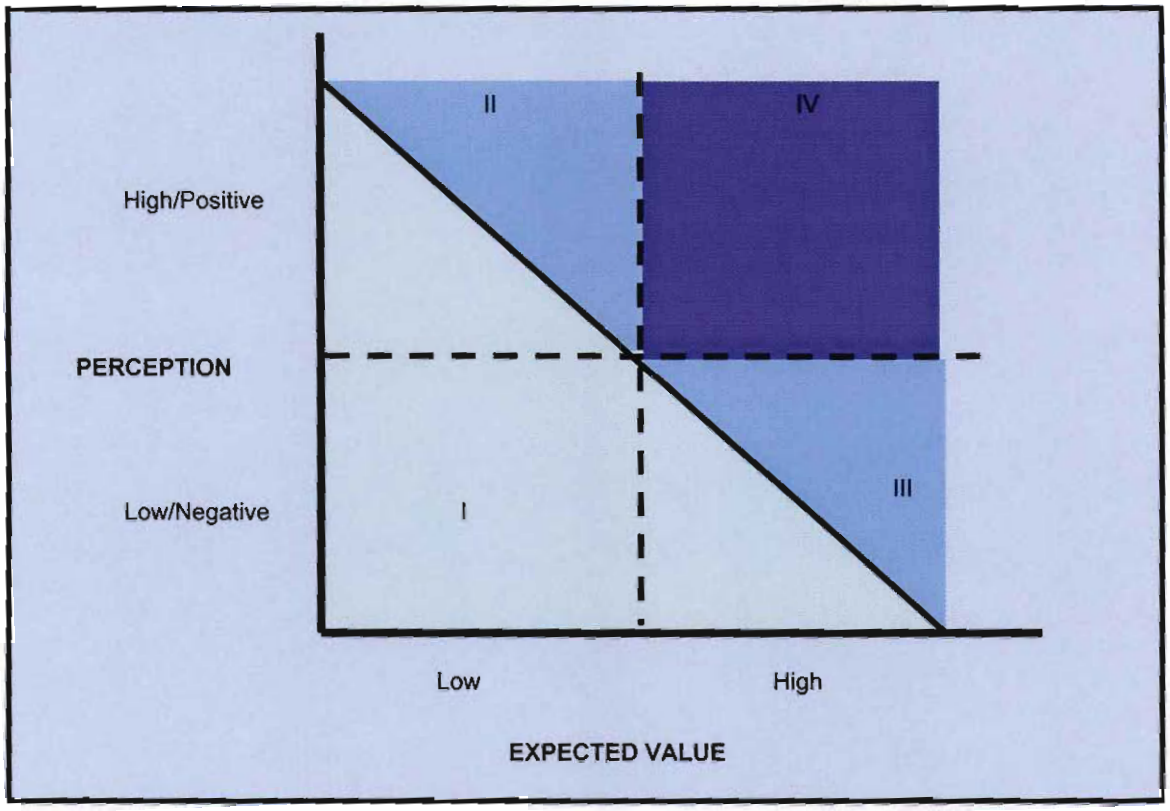
2.6.3.1 Relationship of Confidence, Perception and Quality of Service

The Oxford dictionary meaning of confidence is "an assurance of manner" (OED, 1953:162). Nel's (1993:40) measure of the gap difference between *delivered value of service* and *expected value of service* as the *quality of service*. *Confidence* is the customer's view *(assurance) of the quality of service (manner)*. Hence, confidence can be viewed as a product of customer perception and customer expectation of value i.e.

CALCULATED CONFIDENCE = PERCEPTION X QUALITY OF SERVICE

Security, be it active, controls to ensure trust, or attacks on the system, will influence the state of the elements that influences perception and/or the quality of the service. Using the aforementioned relationship of confidence with respect to perception and quality of service, the following map is compiled:-

Figure 2-9: The Perception Expectation Matrix



Negative sentiment or events drive perception towards zero. Likewise, as the quality of service diminishes due to decay or excessive risk, the quality of service value tends towards zero. This implies that the confidence (i.e. the product of perception and expectation) tends to matrix segment 1. In both instances, confidence diminishes and decay sets in.

The converse, where perception and expected values improve, will apply, i.e. a trend towards matrix segment IV. This result in higher confidence and an expected increase in usage and adoption rate of the channel.

The objective of the study is to improve the confidence of Internet banking by dealing with the issue of security. Figure 2-9, present a matrix that allows one to map confidence (a product of perception and quality of service). The position can then be altered by addressing the issue at hand i.e. one of perception or one of quality of service.

Litan (2006b:2) mentions that phishing attacks have substantially increased in the last two years, indicating a change in trend of attack methods, from the organisation to the customer. The shift is attributed to the strong security controls implemented by organisations to fulfil regulations such as King II and the Payment Card Industry Data Security Standard.

The effect of these attacks on customers has caused behavioural habits to change, as indicated in figure 1-1. Given that the quality of service pertaining to security has improved, one can deduce that perception is affecting confidence; in this case negatively. To mitigate the impact, organisations require changing perception by attending to the factors that influences perception.

2.7 Measuring Perception

Referring to figure 2.7, it is evident that the end result of perception which is judgement and decisions undergoes a process of filtering, processing (encoding and simplification) and storage. These attributes are unique to individuals as they are influence by external environments and their own experiences (Schiffman & Kanuk, 2004:168). The implications of this on measurements is that one cannot have a fixed scale to quantify perception but creating a scoring system that gives a indication to perception.

The Likert scale whereby questions are evaluated on feeling-based responses becomes the appropriate manner to measure perception which translates feeling in the range of strongly agree to strongly disagree to scores of 1 to 5 thereby allowing for the statistical analysis of perception (Survey Monkey, 2007:9)

2.8 Change Management

2.8.1 E-Commerce Change Model

To cushion the disruptive effects of rapid changes to technologies, an organization requires a comprehensive plan that supports agility and flexibility. Lewin's change model of unfreezing, moving and refreezing fails, due to the short technology life cycle of the elements that constitute the environment. Cummings & Worley (2001:24) describes two alternative planned change models, namely, Action Research Model and the Contemporary Action Model.

The e-commerce environment interacts intensely with external users in a rapid evolving space. To match the speed, organisations will require specialist skills to shed light on the characteristics of external users and be able to invoke a change with least impact and with agility. Comparing the two models, i.e. Action Research and Contemporary, the former requires a behavioural expert and involves joint diagnosis and actioning of the change. The latter, i.e. contemporary, is based on a vision with broad participation which implies rigidity to alter in a short time.

The Action Research model comprises of 8 steps of which steps 4 to 8 is a re-assessment loop, ideal to deal with the continuous fluctuation of threats the Internet Landscape is subject to. The steps of the model are:

- Problem Identification
- Consult with Behavioural Science Expert (consumer market specialist)
- Gather data and preliminary diagnosis

- Feedback to business and IT Security tactical group
- Joint Diagnosis of Problem
- Joint Action Planning
- Action
- End-results analysis and review actions

The model suggested above provides a framework to manage the impact of threats on users. Evident from the response to threats is finding the appropriate security control, leading us to manage a dilemma of threats over security controls, similar to the Breathing Polarity (Johnson, 1996:21).

Security controls and threat are both present and will always be present within the environment. As the one increases, the other diminishes and vice versa, in a cyclic manner. The essence to manage this dilemma is to discard the "Either/Or" thinking and adopt a "Both/And" view of the dilemma (Johnson, 1996:24).

To ensure a harmonious change, Coetsee (2006:46) mentions ten principles for successful change management

- Principle 1: Establish what the results of the change process should be - Involves defining what the end result of the change process must be before introducing the change process
- Principle 2: Clarify the need for change - The eventual result of the change process and if this result is desirable must be known before the change occurs.
- Principle 3: Involve and obtain the commitment of all stakeholders in the planning and execution of the change process - Aligned commitment = Information x knowledge x Empowerment x Rewards and recognition x vision

- Principle 4: Diagnose present functioning - "Diagnosis of the present functioning of the organisation is the basis of successful change management"
- Principle 5: Develop a result-oriented rather than an activity-orientated strategy for change - All elements of a strategy must be focused on achieving desired results.
- Principle 6: Assure that enabling structures are all aligned - All aspects of an organisation should be focused and committed to achieving a common goal
- Principle 7: Pay special attention to the organisational culture and climate - The culture and climate of an organisation should be included in the change process
- Principle 8: Create a change-adept Learning organisation - Make Organisational learning and knowledge management permanent within the organisation.
- Principle 9: Diagnose and Manage resistance to change. Resistance arises when change occurs, hence it is imperative that this resistance is identified and made permanent within the organisational structure
- Principle 10: build in reliable feedback mechanism to monitor, manage and eventually evaluate the change process - Regularly collect the relevant information about the change process and the related consequences at every stage of this process

These principles apply to a change audience that is totally under the control of the organisation. In the Internet banking context the end-user (customer) is only under the control of the organisation during the time of interaction. Hence an innovative stance is required so that most of the 10 principles are adhered to during the change process affecting end-users (customers).

2.9 Summary

Technology dependent solution can be positioned in a technology adoption lifecycle model that directs one on the strategy to take, going forward. It takes into account the current environment and the challenges needed to overcome the inflection points. The Internet banking environment is positioned close to maturity with a strategic inclination to move away from standardisation. However the external threat of e-commerce security dictates that the first value-add is to improve security matters. However the same may not be applicable to mobile banking which is "crossing the chasm".

The strategy for mobile banking is to grow the solution in a niche market before adopting a standardisation model. But ignoring security matters may be detrimental and against the philosophy of multi-channel architecture that requires a similar customer experience over related technology solutions. Hence the security matters must be dealt with in conjunction to those for Internet Banking.

Security threats have shifted away from attacks on organisation, to attacks on their customers, resulting in a lack of trust. To mitigate the effects, one may consider a perception strategy that influences the customers' thought processes to re-instate the balance.

Implementing the changes requires managing a dilemma of security controls and threats which is in effect a polarity management issue.

Chapter 3: Empirical Study

3.1 Introduction

The literature study provided the foundation for the objectives that addresses the problem (stated below). The problem is defined to focus on customers and to assess the severity of the problem; two questionnaires were compiled to obtain information on customers' feelings towards Internet banking and mobile banking respectively.

3.2 Statement of the Problem

As stated in sections 2.3, the problems identified are:

- A significant number of Internet banking users have a perception that the security provided by the Internet banking solution is inadequate for their satisfaction.
- Information security attacks and concerns negatively affect the confidence of Internet banking

3.3 Aim of the Empirical Research

The aim of the of the empirical study is to validate the primary objective which was presented (in section 2.6.3.1) as a mathematical formula:

CALCULATED CONFIDENCE = PERCEPTION X QUALITY OF SERVICE

The survey is structure to ask questions that map to perception and quality of service as describe and categorised in table 3.1. These questions related to the factors of perception and quality of service that was previously mentioned in section 2.6.3 and 2.4.3 respectively.

To obtain a calculated confidence, items within the questionnaire will be combined and normalised giving the ***Calculated Confidence (U_1).*** The questionnaire will include questions that related directly to the customers claimed confidence denoted as ***Customer Confidence (U_2)***.

Thus we wish to test the null hypothesis, that there is no difference between the two confidence means, i.e. ***Calculated Confidence (U_1)*** **and** ***Customer Confidence (U_2)*** at a significant level of 1%. We can assume a normal distribution as the sample size is sufficient large to apply the central Limit Theorem, i.e. greater than 30 (Wisniewski, 2002:215-219), i.e.

$$H_0 : (U_1 - U_2) = 0$$
$$H_1 : (U_1 - U_2) \neq 0$$
$$\alpha : 0.01$$
$$Z_\alpha : 2.58$$

where $$Z_{calc} = \frac{(\bar{X}_1 - \bar{X}_2) - (U_1 - U_2)}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

From the results of the survey and the application of the aforementioned formulae, we can validate the correlation of confidence to adoption and usage rate of Internet banking and mobile banking.

The structure of the questionnaires for the survey is designed to branch into four distinct categories:

1) Respondents that uses Internet banking
2) Respondents that do not use Internet banking
3) Respondents that uses mobile banking

4) Respondents that do not use mobile banking

The categories 2 and 4 may contain a significant number of users who do not use the facility currently but may do so in the future. Hence their response may be bias in favour of perception. Therefore the hypothesis test will be restricted to categories 1 and 3, while correlation analysis can be used as these have a definite usage.

The results of the empirical study will provide input for a strategic approach that fulfils the secondary objective:

- A strategy to influence security perception by addressing e-commerce security matters
- A change management strategy for the implementation of security solutions and features that minimise impact to clients
- A proposed fraud management-solution based on individual behavioural habits to reduce financial risk to customer and bank

3.4 Survey Design

3.4.1 Questionnaire Content

The content of the questionnaire is made up of the cover page and 2 sub-sections of questions, one to evaluate Internet banking and the other to evaluate mobile banking.

3.4.2 Covering Page

The intent of the cover page is to introduce the topic to respondent, given a brief description of the objective and instructions for the completion of the survey.

3.4.3 Questions Design

Each questionnaire was set to allow the respondent to branch based on whether the channel evaluated, i.e. Internet banking or mobile banking was used or not.

Thereafter the remaining questions were design to

- evaluate the factors of perception and obtain a aggregate score
- evaluate the quality of service and obtain an aggregate score
- request the respondent to provide a confidence score

Table 3.1 provides a matrix that groups the questions into actual confidence, usage of channel, perception factors or confidence factors allowing for the validation of the hypothesis mentioned in section 3.3 and summarised in Appendix B.

Table 3-1: Question to Factor Matrix

Factor	Factor Type	Channel	Applicable Question
Customer Confidence score	confidence	Internet	Q4, NQ1
		Mobile	Q4, NQ1
Customer Usage	Usage	Internet	Q2, Q3, NQ2, NQ3
		Mobile	Q2, Q3, NQ2,NQ3
Computer Literacy levels and awareness	perception	Internet	Q5, Q6, NQ4, NQ5, NQ6
		Mobile	Q5, Q6, Q7,NQ4, NQ5,
Monetary risks	perception	Internet	Q8, Q9, NQ7, NQ8
		Mobile	Q9, Q10, NG6, NQ7,
Functional risks	perception	Internet	Q10, Q11, NQ15,
		Mobile	Q11, NQ8, NQ15
Changes to the technology environment	perception	Internet	Q12, NQ9
		Mobile	Q12, NQ9
Complexity	perception	Internet	Q7, Q13, NQ10
		Mobile	Q8, Q13, NQ10,
past experience or communication	perception	Internet	Q14, Q15, Q16, Q17, NQ11, NQ12, NQ13, NQ14

		Mobile	Q14, Q15, Q16, Q17, NQ11, NQ12, NQ13, NQ14
Trustworthiness	quality of service	Internet	Q21, Q24, NQ19, NQ21
		Mobile	Q19, Q24, NQ21,
Response times	quality of service	Internet	Q23
		Mobile	Q23
Availability	quality of service	Internet	Q22, NQ17
		Mobile	Q22, NQ19
Reliability	quality of service	Internet	Q20, NQ23
		Mobile	Q20, NQ20
Functional	quality of service	Internet	Q18, Q19, Q25, Q27, Q28, NQ16, NQ18, NQ20, NQ22, NQ24
		Mobile	Q18, Q21, Q25, Q26, Q28, NQ16, NQ22, NQ23
convenience	quality of service	Internet	Q26
		Mobile	Q27
Marketing	Behavioural change	Internet	NQ25,
		Mobile	NQ24
Guarantee against risks	Behavioural change	Internet	NQ26, NQ27, NQ28
		Mobile	NQ 25, NQ26, NQ27
Added value	Behavioural change	Internet	NQ29
		Mobile	NQ28

3.5 Pre-survey Questionnaire Test

The aim of the pre-survey questionnaire test was to get feedback of the questionnaires on its objectiveness, clarity, use and time to complete. The feedback was used to revise the questionnaire to assure a high quality and better reliance on data.

3.6 Survey Overview

The questionnaires were distributed by hand to randomly passing-by individuals at locations that favoured the middle to upper-middle segment, i.e. an the office park situated in Marshalltown, Johannesburg Central Business District and at franchise food outlets in the suburbs of Lenasia and Victory Park (Johannesburg). The rationale to choose these venues was that the people present were totally random, form part of middle to upper middle segment and have time while relaxing or waiting.

A total of 350 questionnaires were distributed.

3.7 Results Overview

As the survey was interactive and not distributed by email post and a physical presence of the surveyor explaining the purpose and what was needed, the response was very positive with 21 rejected/spoilt questionnaires (94% success rate).

Chapter 4: Analysis

4.1 Introduction

The data from the surveys were captured onto a Microsoft Excel worksheet and processed into meaningful statistical information as attached in Appendix B.

The data was separated into the categories based on the hypothesis test namely:

- Respondents that uses Internet banking
- Respondents that do not use Internet banking
- Respondents that uses mobile banking
- Respondents that do not use mobile banking

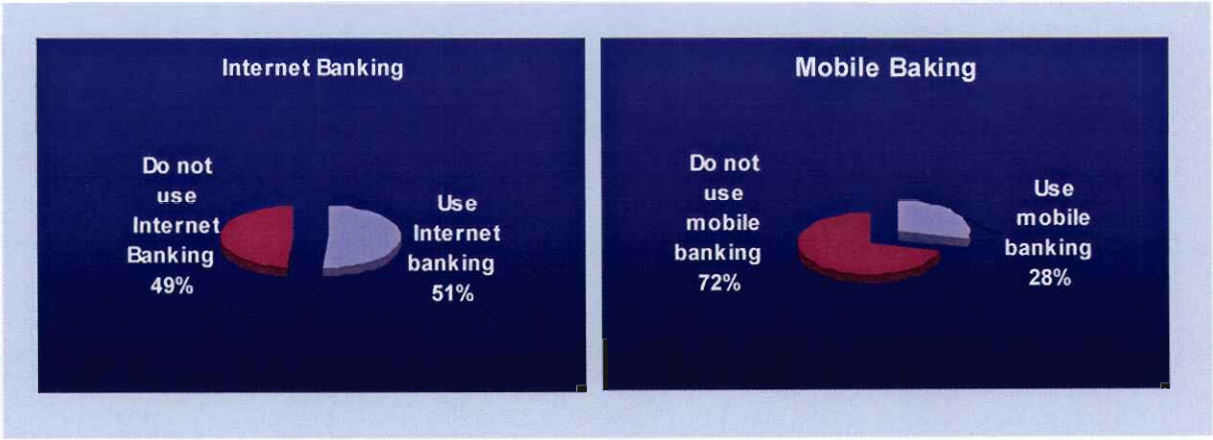
Thus the analysis is segmented into the categories above.

4.2 Analysis of results

4.2.1 Technology Adoption Proportions

The adoption and usage of Internet and Mobile differ significantly as indicated below:

Figure 4-1: Adoption and Usage Proportions



The proportion of Internet banking and mobile banking users that have adopted the technology is in line with the BMI-T (2005) statistic as depicted in figure 2-2 when the 1 year future adoption is applied, i.e. 51 % and 28 % versus 50% and 29 % respectively. This supports the reliability of the response of the survey.

Furthermore, the results of the proportion of Internet banking indicates that the technology solution is at its maturity with the emphasis to gain growth amongst the late majority as previously indicated. However the higher than expect proportion of 29 % for mobile banking indicates that channel has "crossed the chasm" and is achieving the expected growth in adoption.

4.2.2 Validation of Hypothesis

4.2.2.1 Internet banking - "yes" category

Based on the statistical information in Appendix B, the results of the null hypothesis $H_0 : (U_1-U_2) = 0$ as defined in section 3.3, for Internet banking – "yes" category is as follows:

$$Z_{calc} = \frac{(0.695 - 0.561) - (0)}{\sqrt{\frac{0.158^2}{84} + \frac{0.108^2}{84}}}$$

$Z_{calc} = 4.96$, which is greater than $Z_{\alpha} = 2.58$

Hence we reject the null Hypothesis for the Internet banking "yes" category which was derived in section 2.6.3.1 as

Calculated confidence = perception X quality of service.

What is noticeable is the Square root of the calculated confidence seems to be more appropriate. Hence we set a new hypothesis based on the revised formula, i.e.

Calculated confidence = square root of (perception X quality of service)

The new hypothesis is

H'_0 : $(U_1 - U_3) = 0$

H'_1 : $(U_1 - U_3) \neq 0$

ά : 0.01

$Z_{ά}$: 2.58

Where U_1 is the mean of the customer confidence, and U_3 is the mean of the square root of the calculated customer confidence, i.e.

Thus,

$$Z_{calc} = \frac{(0.695 - 0.744) - (0)}{\sqrt{\frac{0.158^2}{84} + \frac{0.073^2}{84}}}$$

Z_{calc} = -0.89, which is less than $Z_{ά}$ = 2.58

We can accept the new null hypothesis, thereby relating

Calculated Confidence = square root of (perception X quality of service).

4.2.2.2 Mobile banking - "yes" category

Based on the statistical information in Appendix B, the results of the null hypothesis $H_0 : (U_1-U_2) = 0$, as defined in section 3.3, for mobile banking – "yes" category is as follows:

$$Z_{calc} = \frac{(0.753 - 0.519) - (0)}{\sqrt{\frac{0.155^2}{47} + \frac{0.140^2}{47}}}$$

$Z_{calc} = 7.68$ which is greater than $Z_{\acute{a}} = 2.58$

Therefore we reject the null Hypothesis for the mobile banking "yes" category which was derived in section 2.6.3.1 as

Calculated confidence = perception X quality of service.

As for the Internet banking, it is noticeable that square root of the calculated confidence seems to be more appropriate. Hence we test for a new hypothesis based on the revised formula, i.e.

Calculated confidence = square root of (perception X quality of service)

The new null hypothesis

H'_0 : $(U_1 - U_3) = 0$

H'_1 : $(U_1 - U_3) \neq 0$

á : 0.01

$Z_{\acute{a}}$: 2.58

Where U_1 is the mean of the customer confidence, and U_3 is the mean of the square of the customer confidence

Thus,

$$Z_{calc} = \frac{(0.753 - 0.710) - (0)}{\sqrt{\frac{0.155^2}{47} + \frac{0.096^2}{47}}}$$

$Z_{calc} = 1.618$, which is less than $Z_{\alpha} = 2.58$

We can accept the new null hypothesis, thereby relating

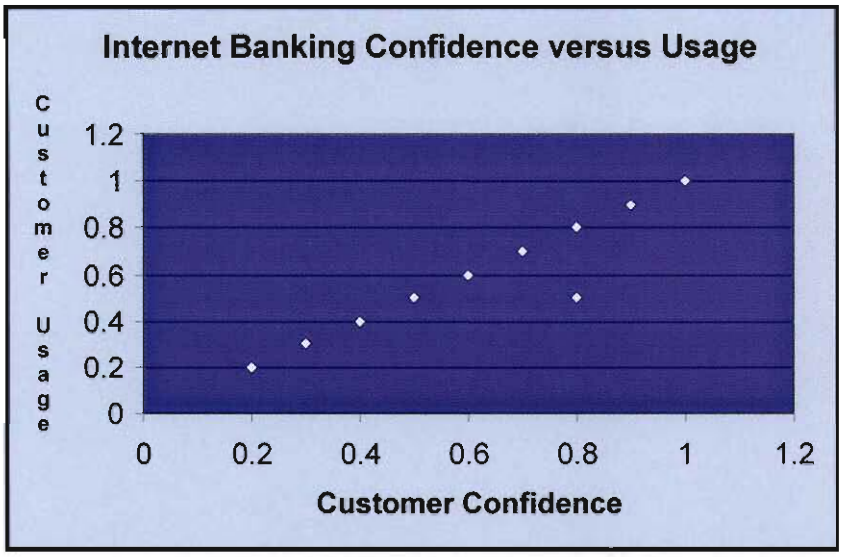
Confidence = square root of (perception X quality of service).

4.2.3 Analysis of Correlation

4.2.3.1 Internet Banking "YES" category

The correlation coefficient (r), which measures the strength of the relationship between two variables, in this instance, customer confidence and customer usage or Internet banking is 0.985 which a almost perfectly correlation (Wisniewski, 2002:326), substantiated by the graph below.

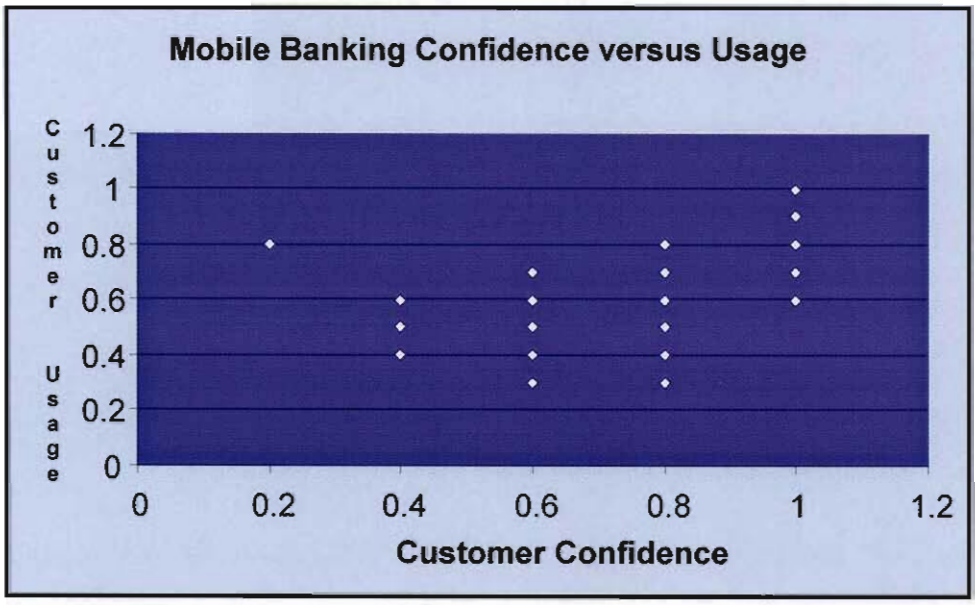
Figure 4-2: Internet Banking Confidence versus Usage relationship



4.2.3.2 Mobile Banking "YES" category

Similarly, using the correlation coefficient (r) for mobile banking, customer confidence and customer usage is 0.436 which signifies a fairly linear relationship, with a positive gradient, i.e. when confidence increase, so will usage (Wisniewski, 2002:326), as depicted by the graph below.

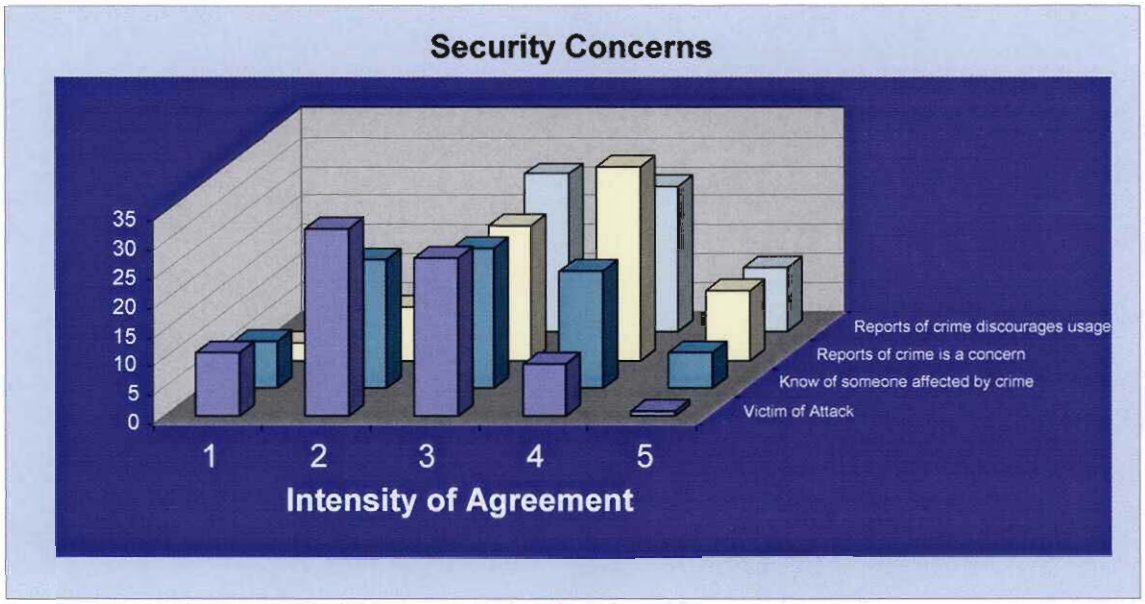
Figure 4-3: Mobile Banking Confidence versus Usage relationship



4.2.4 Analysis of Security Matters – Internet and Mobile Banking "No" responses.

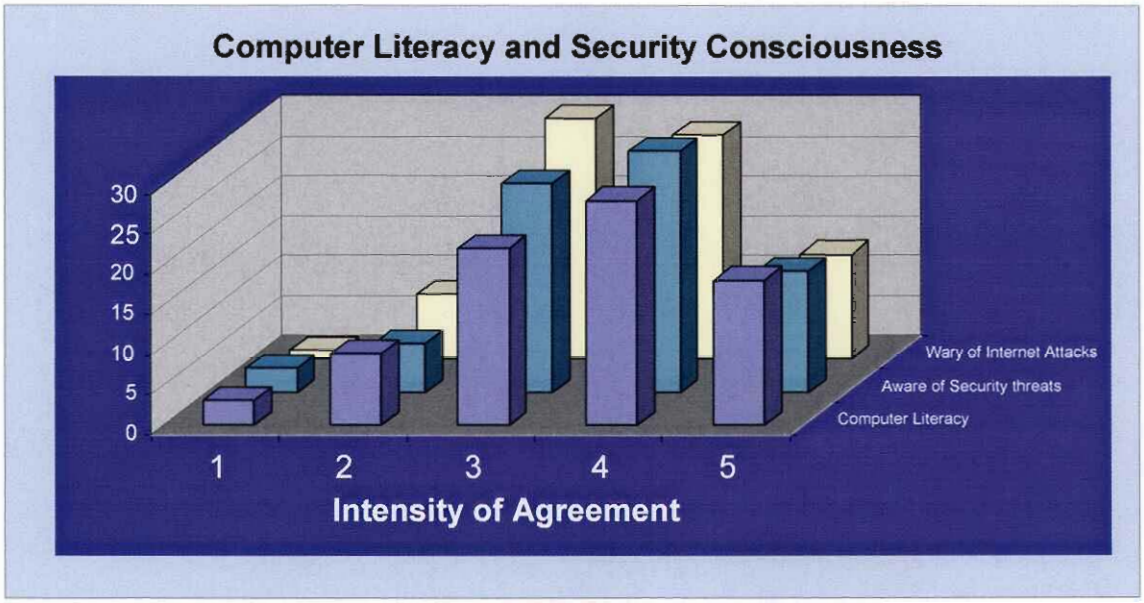
The literature study indicated a shift of cyber crime that was previously aimed at the bank to the customer creating the uncertainty of the sanctity of the platform. The survey revealed a significant number of users were security conscious and will change their behaviour as indicated by below.

Figure 4-4: Security Concerns



Furthermore, security consciousness seems very high as indicated in the figure 4-6. This fact that computer literacy is high and a strong awareness of threats, one can only deduce that the wariness has resulted in the change in behaviour, which is significantly higher.

Figure 4-5: Computer Literacy and Security Consciousness



4.3 Recommendations

The recommendations that follow address the secondary objective of the study.

4.3.1 Influencing Security Perception

The survey clearly indicated the impact security matters have on customers, where, customers become cautious to avoid monetary risk. The perception is further entrenching due to bad news coverage of attacks, knowing of incidents or becoming a victim.

The advantage to the bank is that security awareness is high. To prevent negative sentiment customers feel, the primary focus is to drive an effective education campaign.

The tactical approach is to use the current channels to place "sublime" messages, instilling an "averting the e-crime threat" mind-set. The mind-set must be supported through various mediums namely:

- Industry-wide advertising campaign;
- Broadcasting educational material pertaining to computer literacy and e-commerce security
- Providing tutorials to new users (online from the web site, on CD/DVD)
- Providing education access points at strategic locations e.g. branches

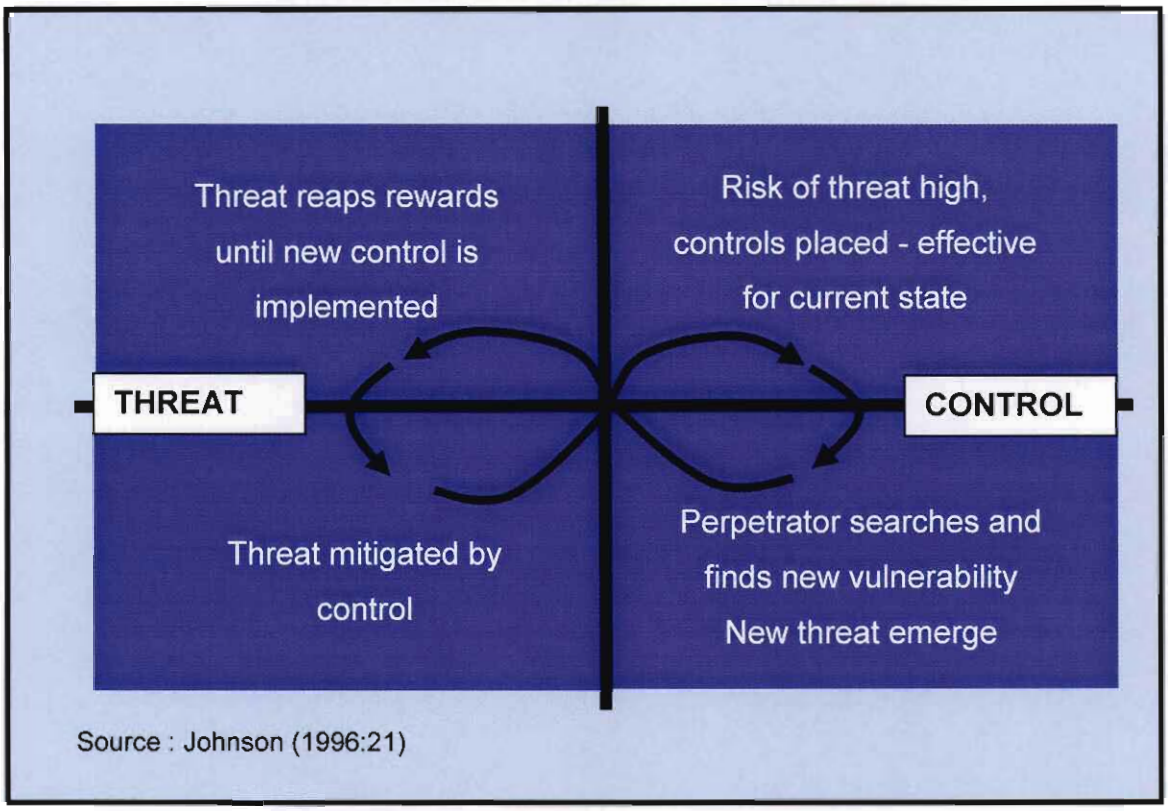
Further consideration must be given to investing in a cyber crime unit that builds relationships with law enforcement authorities to ensure higher conviction rates. The intent is to help contain the growth of e-crime and to improve the negative communication with an active and involved campaign against crime.

The third and final is to evolve the current risk controls of static limits that customer choose on their estimated requirements, e.g. R10000 electronic payment monthly limit, to a dynamic fraud management system that considers customer historical transacting habits to re-calculate and adjust limits. This management system must be able to traverse the various channels within a multi-channel environment, be available during the course of the transactions and report exceptions.

4.3.2 Managing E-Commerce Changes – A Polarity Management Approach

Responding to a threat, is no more than tackling a dilemma. The perpetrator will simple search for the next vulnerability even thought the current control was effective. Hence controls containing the current threat does not guarantee against future. The perpetrator will exploit the new vulnerability; reaping rewards until the threat is mitigated. This cyclic dilemma is similar to the breathing polarity as depicted figure 4-6 (Johnson, 1996:21).

Figure 4-6: E-commerce Control / Threat Polarity



The effective change management strategy is thus,

- Consider the threat and control as dilemmas, both of which will exists
- Position the dilemmas in a polarity map
- Revise the basic risk management (figure 2-5) and security framework model to fit into the polarity
- Adhere to as many as the principles of change management mentioned previously
- Manage communications to customers to avoid panic and promote awareness

4.4 Conclusion

The change management strategy above provides an integrated way to combat e-commerce, involving all stake holders. The result will be an improve perception by both business and customer who will see the initiative as added-value.

Such a strategy addresses both, the mitigation of threats and the maintenance channel integrity. The complexities of the environment expand various business management fields, in particular technology and information management. Having in-depth knowledge of these management areas allows one to formulate effective strategies that keep pace with the rapidly evolving technology world which are presented to customers without the disrupting effect of change.

Change does effect customer perception adversely. Having the tools to influence customer perception does give a organisation the competitive edge – one that promotes confidence that reaps business value through increase usage.

Confidence does increase usage, and confidence is a function of perception and quality of service.

Bibliography

ACTS see SOUTH AFRICA.

Arunachalam, L. & Sivasubramanian, M. 2007. Theoretical Framework To Measure The User Satisfaction In Internet banking. Volume 20. http://www.acadjournal.com/2007/V20/part6/p3/ Date of Access: 10 Oct 2007.

Basel Committee on Banking Supervision. 2005. International Convergence of Capital Measurement and Capital Standards: A Revised Framework. http://www.bis.org/publ/bcbs118.htm Date of Access 15 Sept 2007.

BMI-T. 2005. The changing face of banking in South Africa: Banking Industry Overview. BMI TechKnowledge group.

Burgelman, R. A., Maidique, M. A., & Wheelwright, S. C. 2001 Strategic management of technology and innovation (3rd Ed.) McGraw- Hill. New York.

Buys, R. & Cronje , F. (eds). 2004 Cyberlaw: The law of the Internet in South Africa. Van Schaik Publishers. Pretoria.

Cain, R. 2007. The business case for mobile banking. VRL KnowledgeBank. Patersons. London.

Cazemier, J.A. , Overbeek, P. L. & Peters, L. M.C. 2004 Best practice for security management. The Stationery Office. London.

Coetsee, L. 2006. Change Management: Study Guide for MDTP 815. Potchefstroom: North West University.

Cummings, T.G. & Worley, C. G. 2001 Organization development and change (7th Ed). South- Western College Publishing. USA.

Field, A. 2005 Discovering Statistics Using SPSS (2nd ED.) Sage Publications, London.

Gartner. 2006. Toolkit: Online Banking Needs More Security to Retain Consumers. Gartner, Inc.

Institute of Directors in Southern Africa. 2002. Executive Summary of the King Report 2002: King Committee on Corporate Governance. http://www.corporatecompliance.org/Content/NavigationMenu/International/SouthAfrica/ Date of Access 15 Sept 2007.

Intel. 2007. Moore's Law. http://www.intel.com/technology/mooreslaw/ Date of Access 10 Oct 2007.

Johnson, B. 1996 Polarity management- Identifying and managing unsolvable problems. HRD Press. Massachusetts.

Kreitner, R. & Kinicki, A. 2004 Organisational Behavior (6th International Ed.). McGraw- Hill. New York.

Litan, A. 2006a. How to Evaluate Combined Fraud Detection and Authentication Services. Gartner, Inc., Apr.

Litan, A. 2006b. Phishing Attacks Leapfrog Despite Attempts to Stop Them. Gartner, Inc., Nov.

Macknight, J. 2005/2006. Balls in the air. Banking Technology:12-15, Dec/Jan.

Mitnick, K.D. & Simon, W.L. 2002 The art of deception- controlling the human element of security. Wiley Publishing. Indiana.

Nel, D. 1993. Service quality in a retail environment: closing the gaps. Journal of General Management, 18(3): 37-45, Spring.

O'Brien, J.A. 2007. Management Information Systems: Managing Information Technology in the Business Enterprise (6th Ed). McGraw Hill Irwin. Boston.

OED (Oxford English Dictionary) 1953. "Perception". Oxford: At the Clarendon Press.

PCI Security Standard Council. 2006. Payment Card Industry(PCI) Data Security Standard. https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm Date of Access 15 Nov 2006.

Pickett, K. H. S., 2006 Enterprise Risk Management- A Manager's Journey. John Wiley & Sons. New Jersey.

Schiffman, L G. Kanuk, L L. 2004 Consumer behaviour (8th Ed). Prentice-Hall. New York.

Schneider, G. P. 2007 Electronic Commerce (7th Annual Ed). Thompson Course Technology. Canada.

Selame, E. 1997. What's in a name? Bank Marketing, 29(2):15-20, Feb.

Shibayama, S. 2007. Metcalfe's Law. http://www.searchnetworking.techtarget.com/sDefinition/ Date of Access 10 Oct 2007.

Simon & Shuster. 2001. The Twenty Laws of the Telecosm. http://www.kurzweilai.net/articles/art0004.html?printable=1 Date of Access 10 Oct 2007.

Sklar, D. 2001. Building trust in an Internet economy. Strategic Finance:22-25, Apr.

SOUTH AFRICA. 1990. Banks Act 94 of 1990. Pretoria: Government Printer.

SOUTH AFRICA. 2001. Financial Intelligence Centre Act 38 of 2001. Pretoria: Government Printer.

SOUTH AFRICA. 2005. Electronic Communications Act 36 of 2005. Pretoria: Government Printer.

Stenzel, J., Cokins G., Flemming B., Hill, A., Hugos, M., Niven, P., Schubert, K., & Stratton A. 2007. CIO best practices: enabling strategic value with information technology. John Wiley & Sons. New Jersey.

Stewart, A. 2004. On risk: perception and direction. Computer & Security, 5:362-370, Jul.

Survey Monkey. 2007. Smart Survey Design.

http://www.surveymonkey.com/HelpCenter/AskQuestion.aspx Date of Access 12 Sept 2007.

Trout, J. 2004. Trout on strategy: capturing mindshare, conquering markets. McGraw-Hill. New York.

Van Buuren, R. 2006. The competitive revolution: ten forces facing global business. Management Today, 22(1):36-38, Feb.

Von Solms, B. 2003. Governance, risk & ethics: module 7: information technology governance & risks. Financial Mail, 1-8, 20 Jun.

Von Solms, B. & Von Solms, R. 2004. The 10 deadly sins of information security management. Computers & Security, 5:371-376, Jul.

Von Solms, R. 1996. Information security management: the second generation. Computers & Security, 15(4): 281-288.

Walker, R. & Johnson, L. W. 2005. Towards understanding attitudes of consumers who use Internet banking services. Journal of Financial Services Marketing, 10(1):82-94, Nov.

Wisniewski, M. 2002 Quantitative methods for decision makers (3rd Ed.) Prentice Hall. Harlow, England.

White, H. & Nteli, F. 2004. Internet banking in the UK: why are there not more customers?. Journal of Financial Services Marketing, 9(1):49-56, Sept.

Whiteman, M. E., & Mattord, H. J. 2003 Principles of information security. Thomson Course Technology. Canada.

Appendix A – Questionnaire

The content that follows is the questionnaire that was distributed for the survey.

Good Day

I am a Master Student at the University of the North West and require completing a mini-dissertation to fulfil the requirements of the course.

I have chosen a topic that relates to customer perception of the Internet and Mobile (Cell Phone) Banking channel with the objective to recommend changes that will be beneficial to both the customers and banks.

Please allow me some of your time by completing the survey attached.

The survey contains to separate sections:-

- The evaluation of Internet Banking
- The evaluation of Mobile Banking

Please complete both, noting the skip option on the reverse if your do not use either of the channels.

Thank you

Kind Regards

Fayaaz

Evaluation of Mobile (Cell Phone/SMS) Banking

For each question please tick one of the boxes

1	Do you use Mobile (Cell Phone) Banking?	
	YES	NO

If YES, please continue. If NO, please complete the NO section.

2	How often do you use Mobile (Cell Phone) Banking				
	Daily (more than once)	Once Daily	A few times a week	A few times every two weeks	A few times a month
3	Mobile (Cell Phone) Banking is my preferred means of banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
4	I am very confident about using Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
5	I know the features of my cell phone very well				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
6	Mobile (Cell Phone) Banking is free from security attacks				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
7	Mobile (Cell Phone) Banking is marketed well				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
8	Mobile (Cell Phone) Banking is easy to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
9	Mobile (Cell Phone) Banking is safe to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
10	There are risks of fraud when using Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
11	Mobile (Cell Phone) Banking provides most of my banking needs				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
12	Changes to the Mobile (Cell Phone) technologies affect me				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
13	I use my Mobile (Cell Phone) phone freely				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
14	I have been a victim of a malicious Mobile (Cell Phone) attack				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
15	I lost, or know someone personally who lost, money using Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

16	Fraud on Mobile (Cell Phone) Banking is not possible, which increases my confidence in Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
17	News reports of fraud on Mobile (Cell Phone) phones have caused me to change my Mobile (Cell Phone) Banking behaviour				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
18	Mobile (Cell Phone) Banking has most of the functions that I require for banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
19	Mobile (Cell Phone) Banking is trustworthy				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
20	Mobile (Cell Phone) Banking is very reliable				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
21	Mobile (Cell Phone) Banking saves me time by avoiding a branch visit				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
22	Mobile (Cell Phone) Banking is always available when I need to use it				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
23	The response times of Mobile (Cell Phone) Banking are acceptable				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
24	My banking information, such as account balances and statements, are confidential				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
25	Mobile (Cell Phone) Banking is easy to navigate				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
26	Mobile (Cell Phone) Banking can be personalised to suit me				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
27	Mobile (Cell Phone) Banking can be used anywhere, at anytime				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
28	Mobile (Cell Phone) Banking is cost-effective				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

Evaluation of Mobile (Cell Phone) Banking (NO)

(I do not use Mobile Banking)

1	I do not have confidence in Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
2	I have never used Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
3	I have not heard of Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

4	Mobile (Cell Phone) Banking can be affected by of computer viruses, Trojans or phishing attacks				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
5	I am very wary of using Mobile (Cell Phone) Banking because of no privacy				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
6	Mobile (Cell Phone) Banking is safe to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
7	There is a no guarantee against fraud if I use Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
8	Mobile (Cell Phone) Banking may not cater for all my needs				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
9	The Mobile (Cell Phone) environment constantly changes, affecting my attitude towards the Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
10	Mobile (Cell Phone) Banking is too complex to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
11	I have been a victim of a malicious attack relating to a Mobile (Cell Phone) phone causing be to doubt its safety				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
12	I lost, or know someone personally who lost, money on the Mobile (Cell Phone) network due to fraud				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
13	News reports of fraud on the Mobile (Cell Phone) network have discouraged me from using Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
14	News reports of fraud on the Internet have discouraged be from using Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
15	I prefer a branch visit instead of Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
16	Mobile (Cell Phone) Banking does not have the functionality of my banking needs				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
17	I doubt that Mobile (Cell Phone) Banking is available 24 hours a day, 7 days a week				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
18	Mobile (Cell Phone) Banking is not trustworthy				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
19	Mobile (Cell Phone) Banking is unreliable				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

20	I doubt the cell phone network's reliability, which may disrupt communication				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
21	My banking information, such as account balances and statements, are not confidential				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
22	Mobile (Cell Phone) Banking is not cost -effective				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
23	I have no need for Mobile (Cell Phone) Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
24	I will consider using Mobile (Cell Phone) Banking if I know more about it				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
25	I will consider using Mobile (Cell Phone) Banking if It is guaranteed safe to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
26	I will consider using Mobile (Cell Phone) Banking if there is insurance against losses due to fraud				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
27	I will consider using Mobile (Cell Phone) Banking if there is a personalised fraud management feature				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
28	I will consider using Mobile (Cell Phone) Banking if it is promoted as a value-added service				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

Evaluation of Internet Banking

For each question please tick one of the boxes

1	Do you use Internet Banking?	
	YES	NO

If YES, please continue. If NO, please complete the reverse.

2	How often do you use Internet Banking				
	Daily (more than once)	Once Daily	A few times a week	A few times every two weeks	A few times a month
3	Internet Banking is my preferred means of banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
4	I am very confident about using Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
5	I have adequate computer literacy skills				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
6	I am aware of computer viruses, Trojans and phishing attacks				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
7	Internet Banking is simple to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
8	Internet Banking is safe to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
9	There are sufficient controls to guarantee that there is no loss due to fraud				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
10	Internet Banking provides most of my banking needs				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
11	I feel comfortable using Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
12	Changes to the Internet environment affect me				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
13	I use the Internet freely, ignoring items that do not interest me				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
14	I have been a victim of a malicious Internet attack				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
15	I lost, or know someone personally who lost, money on the Internet due Internet fraud				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
16	News reports of fraud on the Internet are of concern to me				

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
17	News reports of fraud on the Internet have caused me to change my Internet banking behaviour				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
18	Internet banking has most of the functions that I require for banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
19	Internet Banking saves me time by avoiding a branch visit				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
20	Internet Banking is very reliable				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
21	Internet Banking is trustworthy				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
22	Internet banking is always available when I need to use it				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
23	The response times of Internet banking are acceptable				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
24	My banking information, such as account balances and statements, are confidential				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
25	The Internet Banking site is easy to navigate				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
26	Internet Banking can be used anywhere at anytime				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
27	There is a comprehensive help function on the use of Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
28	Internet Banking is cost-effective				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

Evaluation of Internet Banking (NO)

(I do not use Internet Banking)

1	I do not have confidence in Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
2	I have never used Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
3	I may use Internet Banking in the future				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
4	I have adequate computer literacy skills				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
5	I am aware of computer viruses, Trojans and phishing attacks				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
6	I am very wary of Internet attacks such as viruses, Trojans and phishing attacks				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
7	Internet Banking is safe to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
8	There is a guarantee against fraud if I use Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
9	The Internet environment constantly changes, affecting my attitude towards the Internet				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
10	Internet Banking is too complex to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
11	I have been a victim of a malicious Internet attack				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
12	I lost or know someone personally who lost money on the Internet due Internet fraud				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
13	News reports of fraud on the Internet are of concern to me				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
14	News reports of fraud on the Internet has discourages be from using Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
15	I prefer a branch visit instead of Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
16	Internet Banking do not have the functionality of my banking needs				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
17	I doubt that Internet Banking is available 24 hours a day, 7 days a week				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

28	I doubt the Internet connectivity which may disrupt communication				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
19	My banking information, such as account balances and statements, are not confidential				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
20	Internet Banking is not cost-effective				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
21	Internet Banking is not trustworthy				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
22	I have no need for Internet Banking				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
23	Internet Banking is unreliable				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
24	Internet Banking does not have a comprehensive help function				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
25	I will consider using Internet Banking if I know more about the Internet				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
26	I will consider using Internet Banking if It is guaranteed safe to use				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
27	I will consider using Internet Banking if there is insurance against losses due to fraud				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
28	I will consider using Internet Banking if there is a personalised fraud management feature				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
29	I will consider using Internet Banking if I have access to the Internet				
	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

Appendix B

Internet Banking "Yes" Response Information Sheet

Notes:

1 N=84
2 Q1 – Use Internet banking (Yes/No)
3 Q2..Q3 – Indication of Customer Usage
4 Q4 – Indication of Customer Confidence
5 Q5..Q17 – Questions pertaining to factors of perception
6 Q18..Q28 – Questions pertaining to factors of quality of service
7 Customer Confidence % - Normalised to a percentage
8 Customer Usage % - Normalised to a percentage
9 Perception % - The aggregate of Q5..Q17 normalised to a percentage
10 Quality of Service % – The aggregate of Q18..Q28 normalised to a percentage

Description	Mean	Std Dev	Number 1's	Number 2's	Number 3's	Number 4's	Number 5's	Median	Quartile 1	Quartile 3	Customer confidence correlation to
Q1											
Q2	2.738	1.193	25	9	26	11	13	3	1	4	
Q3	4.179	0.665	1	3	10	36	34	4	4	5	
Q4	4.048	0.522	0	3	13	45	23	4	4	5	
Q5	4.167	0.595	1	4	5	44	30	4	4	5	
Q6	4.107	0.595	2	3	7	44	28	4	4	5	
Q7	4.107	0.468	1	3	4	54	22	4	4	5	
Q8	3.536	0.910	1	18	15	35	15	4	3	4	
Q9	3.286	0.918	2	22	20	30	10	3	2	4	
Q10	4.000	0.452	1	3	10	51	19	4	4	4	
Q11	4.048	0.408	0	3	8	55	18	4	4	4	
Q12	3.524	0.791	4	9	18	45	8	4	3	4	
Q13	3.786	0.668	1	8	14	46	15	4	3	4	
Q14	2.155	0.705	20	42	13	7	2	2	2	3	
Q15	2.667	1.048	16	26	19	16	7	3	2	4	
Q16	4.119	0.545	2	3	4	49	26	4	4	5	
Q17	3.429	0.888	3	15	20	35	11	4	3	4	
Q18	4.036	0.482	0	3	12	48	21	4	4	5	
Q19	4.440	0.546	0	1	2	40	41	4	4	5	
Q20	3.857	0.656	0	7	17	41	19	4	3	4	
Q21	3.524	0.807	0	14	24	34	12	4	3	4	
Q22	3.798	0.727	2	9	11	44	18	4	3	4	
Q23	3.738	0.572	1	8	10	58	7	4	4	4	
Q24	3.905	0.805	4	5	14	33	28	4	3	5	
Q25	4.012	0.400	0	4	8	55	17	4	4	4	
Q26	3.917	0.583	0	8	10	47	19	4	4	4	
Q27	3.571	0.752	1	9	26	37	11	4	3	4	
Q28	3.452	0.940	7	11	14	41	11	4	3	4	
Customer Confidence %	0.695	0.158									
Customer Usage %	0.692	0.159									0.985
Perception %	0.722	0.064									0.396
Quality of Service %	0.768	0.090									0.362
Perception X quality	0.561	0.108									0.415
Sqrt (perception X quality)	0.744	0.073									0.408

Internet Banking "No" Response Information Sheet

Notes:

11 N=80

12 Q1..Q15 – Questions pertaining to factors of perception

13 Q16..Q29 – Questions pertaining to factors of quality of service

Description	Mean	Std Dev	Number 1's	Number 2's	Number 3's	Number 4's	Number 5's	Median	Quartile 1	Quartile 3
Number			1	2	3	4	5			
Q0										
Q1	3.538	0.893	3	12	18	33	14	4	4	4
Q2	3.725	0.853	4	8	13	36	19	4	4	4
Q3	3.513	0.787	1	10	27	31	11	4	4	4
Q4	3.613	0.896	3	9	22	28	18	4	4	4
Q5	3.600	0.825	3	6	26	30	15	4	4	4
Q6	3.550	0.786	1	8	30	28	13	4	4	4
Q7	2.913	0.814	7	21	29	18	5	3	4	4
Q8	2.938	0.759	6	20	32	17	5	3	4	4
Q9	3.450	0.808	5	7	22	39	7	4	4	4
Q10	3.177	0.805	4	16	24	32	3	3	4	4
Q11	2.463	0.772	11	32	27	9	1	2	3	3
Q12	2.925	0.894	8	22	24	20	6	3	4	4
Q13	3.525	0.834	3	9	23	33	12	4	4	4
Q14	3.300	0.905	6	11	27	25	11	3	4	4
Q15	3.325	0.992	6	15	18	29	12	4	4	4
Q16	3.063	0.730	5	16	30	27	2	3	4	4
Q17	2.913	0.837	7	22	24	25	2	3	4	4
Q28	3.150	0.745	4	14	34	22	6	3	4	4
Q19	2.938	0.980	12	17	21	24	6	3	4	4
Q20	3.100	0.828	8	12	31	22	7	3	4	4
Q21	3.175	0.881	7	13	27	25	8	3	4	4
Q22	3.088	0.834	7	15	28	24	6	3	4	4
Q23	2.925	0.730	7	17	35	17	4	3	4	4
Q24	2.913	0.608	7	12	45	13	3	3	3	3
Q25	3.350	0.893	4	13	25	27	11	3	4	4
Q26	3.638	0.851	4	5	24	30	17	4	4	4
Q27	3.725	0.889	5	6	16	32	21	4	5	5
Q28	3.638	0.876	3	8	22	29	18	4	4	4
Q29	3.400	0.935	3	13	24	25	14	3	4	4

Mobile Banking "Yes" Response Information

Notes:

14 N=47
15 Q1 – Use mobile banking (Yes/No)
16 Q2..Q3 – Indication of Customer Usage
17 Q4 – Indication of Customer Confidence
18 Q5..Q20 – Questions pertaining to factors of perception
19 Q21..Q28 – Questions pertaining to factors of quality of service
20 Customer Confidence % - Normalised to a percentage
21 Customer Usage % - Normalised to a percentage
22 Perception % - The aggregate of Q5..Q20 normalised to a percentage
23 Quality of Service % – The aggregate of Q21..Q28 normalised to a percentage

Description	Mean	Std Dev	Number 1's	Number 2's	Number 3's	Number 4's	Number 5's	Median	Quartile 1	Quartile 3	Customer confidence correlation to
Number											
Q1											
Q2	2.532	1.114	15	6	16	6	4	3	1	3	
Q3	3.574	0.903	0	8	15	13	11	4	3	4	
Q4	3.766	0.777	1	4	11	20	11	4	3	4	
Q5	3.936	0.651	0	5	6	23	13	4	4	5	
Q6	3.149	0.950	2	14	13	11	7	3	2	4	
Q7	3.277	1.122	2	16	5	15	9	4	2	4	
Q8	3.936	0.654	2	2	6	24	13	4	4	5	
Q9	3.362	1.035	1	14	8	15	9	4	2	4	
Q10	3.681	0.790	1	5	11	21	9	4	3	4	
Q11	3.660	1.001	1	9	9	14	14	4	3	5	
Q12	3.447	0.825	3	4	14	21	5	4	3	4	
Q13	3.872	0.812	1	4	10	17	15	4	3	5	
Q14	2.255	0.837	12	18	12	3	2	2	2	3	
Q15	2.383	0.898	10	19	12	2	4	2	2	3	
Q16	2.851	0.882	2	20	13	7	5	3	2	4	
Q17	2.915	0.949	4	16	12	10	5	3	2	4	
Q18	3.617	0.908	0	9	11	16	11	4	3	4	
Q19	3.404	0.898	0	11	14	14	8	3	3	4	
Q20	3.638	0.884	0	8	12	16	11	4	3	4	
Q21	4.213	0.670	0	1	8	18	20	4	4	5	
Q22	3.809	0.771	1	4	10	20	12	4	3	5	
Q23	4.638	1.972	0	7	10	18	11	4	3	5	
Q24	3.809	0.865	1	7	6	19	14	4	3	5	
Q25	4.043	0.611	0	2	9	21	15	4	4	5	
Q26	3.660	0.888	1	7	10	18	11	4	3	4	
Q27	3.936	0.566	0	3	8	25	11	4	4	4	
Q28	3.681	0.806	1	4	14	18	10	4	3	4	
Customer Confidence %	0.753	0.155									
Customer Usage %	0.611	0.140									0.436
Perception %	0.657	0.074									0.453
Quality of Service %	0.772	0.129									0.458
Perception X Quality	0.519	0.145									0.492
Sqrt (perception X quality)	0.710	0.096									0.506

Mobile Banking "No" Information Sheet

Notes:

24 N=118

25 Q1..Q15 – Questions pertaining to factors of perception

26 Q16..Q27 – Questions pertaining to factors of quality of service

Description	Mean	Std Dev	Number 1's	Number 2's	Number 3's	Number 4's	Number 5's	Median	Quartile 1	Quartile 3
Number			1	2	3	4	5			
Q0										
Q1	3.568	0.888	4	12	41	35	26	4	3	4
Q2	4.008	0.723	3	8	17	47	43	4	4	5
Q3	2.780	1.151	18	46	10	32	12	2	2	4
Q6	3.500	0.763	2	12	44	45	15	4	3	4
Q7	3.398	0.859	4	18	40	39	17	3	3	4
Q8	2.941	0.695	9	25	58	16	10	3	2	3
Q9	3.508	0.780	2	12	45	42	17	4	3	4
Q10	3.466	0.695	3	8	47	51	9	4	3	4
Q11	3.475	0.738	4	8	46	48	12	4	3	4
Q12	3.169	0.845	6	26	38	38	10	3	2	4
Q13	2.619	0.827	16	37	46	14	5	3	2	3
Q14	2.619	0.837	16	38	46	11	7	3	2	3
Q15	3.136	0.846	7	26	40	34	11	3	2	4
Q16	3.246	0.881	8	20	37	41	12	3	3	4
Q17	3.331	0.856	6	17	42	38	15	3	3	4
Q18	3.314	0.624	1	11	64	34	8	3	3	4
Q19	2.864	0.819	12	30	44	26	6	3	2	4
Q4	3.291	0.722	5	11	57	33	11	3	3	4
Q5	3.136	0.673	7	15	57	33	6	3	3	4
Q20	3.415	0.725	2	13	47	46	10	3	3	4
Q21	3.203	0.882	11	16	42	36	13	3	3	4
Q22	3.229	0.640	4	11	67	26	10	3	3	4
Q24	3.466	0.737	2	12	45	47	12	4	3	4
Q25	3.424	0.772	1	16	48	38	15	3	3	4
Q26	3.559	0.763	0	12	47	40	19	4	3	4
Q27	3.551	0.764	1	10	49	39	19	3	3	4
Q26	3.559	0.721	0	9	51	41	17	3	3	4
Q27	3.542	0.712	0	10	49	44	15	4	3	4