ANALYSIS OF THE FINANCIAL INSTITUTIONS' STRATEGIC E-BUSINESS SECURITY SOLUTIONS: TECHNICAL AND NON-TECHNICAL

Norman Tinyiko Baloyi

ISACA, ISC2

Box 28289 Sunnyside 0132

ntbaloyi@netscape.net

27 12 678 7575

ABSTRACT

Many financial institutions are now realizing that information technology is enabling business, not just supporting it. For this reason, financial sectors are changing the way they operate to capitalize on this trend by conducting their day-to-day business operations, namely, business-to-business (B2B) and business-to-consumer (B2C) using online applications. The proliferation of e-business and the widespread distribution of systems have created significant challenges for managing security and availability of systems. These challenges result out of a lack of uniformity and integration in the management of information across heterogeneous systems and locations.

To address e-business challenges, an in-depth literature review was conducted to analyse the financial institutions in South Africa using existing models. Industry Analysis model was used as the underlying model in analysing the financial industry forces that are rapidly changing due to new emerging online technologies and intermediaries that are instrumental in driving these changes. Competitor analysis model was used to understand how financial banking and insurance institutions secure their e-business.

E-business strategies such as B2Bs and B2Cs require extensive system integration. To achieve the value proposition these strategies provide, financial institutions need to knit together many systems to provide secure enablement. In this study, an integrated framework approach is applied since the concept of integrated security is emerging as an effective approach to address the new challenges facing e-business.

KEY WORDS

E-business, business-to-business, business-to-consumer, financial institution, industry analysis, competitor analysis, information system, personal identification number (PIN), keypad, public key infrastructure (PKI)

ANALYSIS OF THE FINANCIAL INSTITUTIONS' STRATEGIC E-BUSINESS SECURITY SOLUTIONS: TECHNICAL AND NON-TECHNICAL

1 INTRODUCTION

The financial services market in South Africa is an overcrowded market in which the banking industry is dominated by the "Big Four": ABSA, FirstRand, Nedcor and Standard Bank, followed closely by Investec and BoE. These banks account for over 90% of retail market. Approximately 90% foreign banks are wholly focused on merchant banking and the investment completes the picture (Baloyi, 2005). The insurance industry is dominated by four major companies, Old Mutual, Sanlam, Liberty Life, and Momentum. This insurance industry has been characterised by mergers and take-overs.

Financial institutions have conducted their business online since the late 1960s through closed, private networks (Deloitte & Touché, 2002). Online financial services include banking, brokerage, life and other retail insurance, retirement and estate planning, funds provision, mortgages, credit cards, and much more. In today's business environment, financial institutions potentially deal with millions of customers, many of whom they may never even see face to face. The winning financial services providers may ultimately be those which can provide a one-stop service and which can draw on their customers database more efficiently and effectively to support cross-selling.

Many financial institutions are now realizing that information technology is enabling business, not just supporting it. For this reason, financial sectors are changing the way they operate to capitalize on this trend by conducting their day-to-day business operations, namely, business-to-business (B2B) and business-to-consumer (B2C) using online applications. B2B deals with the type of transactions between businesses using Internet as a commercial medium. B2C deals with the transactions between business and consumers which involve electronic payment. In terms of e-commerce, B2B transaction is more likely to give rise to the incidence of procurement fraud whereas B2C transaction is more likely to give rise to losses caused by credit card fraud, identity fraud, and the consequential charge backs imposed upon businesses by credit card companies (Philippsohn and Thomas, 2003).

As organizations rush to build and support e-commerce applications there is an increasing realization that information and financial assets are becoming more vulnerable to attack (Lichtenstein, 2000). The confirmation of this is that Visa, Mastercard, Discover Financial Services and American Express have admitted that they have all had credit card data compromised (Computer Fraud & Security, March 2003). This is the reason why consumers are concerned by the security and accuracy of electronic information held by third parties because of the perceived ease of access.

For the highest standards of service and convenience, these consumers require secure Web access to companies' back-office systems to assess their status, make purchases, and much more. Enterprises must earn the trust of their customers, their business partners and the regulators. As such, security and technology will be the key in open electronic communities. Attempting to build this trusted or secure e-Business environment will require hard work and can be very time consuming. One slip can cause damage well beyond any immediate economic loss.

The challenge is to ensure that security solutions are not used as a stand-alone solution but they are integrated to provide an economic and effective solution. When managed properly, this integrated solution can provide a sound basis to deploy new services quickly to support changing business

processes, volumes and customer expectations. This paper starts by identifying major risks and their countermeasures faced by financial institutions (section 2), analyses the secure e-business solutions in the financial institutions (section 3) and provides the process-oriented approach into securing e-business (section 4). Future research and conclusions conclude the paper.

2 MAJOR RISKS FACED BY FINANCIAL INSTITUTIONS

Financial institutions are faced with different types of risks that can severely impact the efficient and effective operations of the business. These risks are: theft of customer identity by employees, identity theft, credit card fraud, business interruption, insufficient internal staff training, internal staff compromise, inadequate customer education and awareness, breaches of legislation, and Web spoofing (Baloyi, 2005). This section discusses these risks and countermeasures.

2.1 Theft of customer identity / information by employees

Most computer fraud is committed from within the organization (Bequai, 1998), because opportunities are presented through lax security. Customer data is extremely valuable to criminals and competitors and can be stolen by internal staff for personal gain or selling to competitors. The possibility of theft is due to hacking or security control loopholes. Theft of customer information is expensive to recover and repair since it contains reputation damage and loss of customer confidence. Deterrence measures and culture of security consciousness and respect can reduce malicious behaviour of the employees. Deterrence measures are attempts to discourage people from criminal behaviour through fear of sanctions. Sanctions are effective if people know that they will definitely be punished for the crime or anti-social acts and that the punishment will be harsh. In the context of information systems (IS) security, deterrence efforts are policy statements and guidelines on legitimate use of IS assets, security briefings on the consequences of illegitimate use of IS assets, and audits on the use of IS assets. Visible deterrent efforts (e.g. writings on notice boards or after signing on computer systems etc.) are effective active measures that can reduce IS abuses by convincing potential abusers that the probability of getting caught is high. Deterrence efforts are particularly effective if the punishment for IS abuses is also severe.

2.2 Identity theft

In identity theft risk, a fraudster utilizes sophisticated software to record keystrokes on a customer's personal computer, which sends customers' information to the fraudster, enabling the fraudster to analyse the sent information and identify possible access to account numbers and PINs. Using this information, the fraudster can then signs on to Internet Banking as a legitimate customer and defraud the customer. This was the case with ABSA bank fraudster in 2003 (Granova and Eloff, 2004), where the spyware software was attached to an email and defrauded R530,000 of 10 ABSA clients. In 2002, the personal computers of 21 customers of Development Bank of Singapore, Singapore's largest bank with 370 000 online banking customers, were breached on the same day to obtain PINs and IDs (Computer Fraud & Security, September 2002). All victims were compensated but the bank stated that it may not compensate customers in the future if they are not responsible for the security of their individual PCs. To counteract identity theft, customers should not open suspicious or unfamiliar emails and they should ensure the use of latest anti-virus software. Financial institutions should make keypads available for the customers to combat identity fraud.

2.3 Credit card fraud

Identities are stolen from the net when hackers break into websites and obtain personal information on customers. These hackers then open new credit and bank accounts using those stolen identity. The most common kind of credit card fraud is called *skimming* (Philippsohn and Thomas, 2003). Using skimming technique, the fraudster may use pocket-sized device with a scanning slot to swipe

customers' card. The device makes a copy of the information held on the magnetic strip that are downloaded to a machine and then copied on to a counterfeit card. To prevent credit card fraud, digital signatures should be used.

2.4 Business interruption

Financial institutions like any other business sector is subject to system failures, denial of service attack by hackers or other catastrophic events leading to prolonged unavailability of Internet services. This can result in customer complaints, loss of faith in financial service and regulatory censure. Adequate contingency procedures should be in place.

2.5 Insufficient internal staff training

Financial institution deals with different kinds of clients needing different kinds of services. Some of the services are advisory and data capturing, whereby wrong information to the clients and incorrect capturing, alteration, destruction or misappropriation of data can be costly to repair. Insufficient training of staff can also result in errors that can be costly to the organization. Staff should be well equipped before they can effectively help customers. Instead of only focusing training on the functionalities and procedures, fraud awareness or prevention, risk management and incident handling can also add to the necessary knowledge of financial institution's internal staff.

2.6 Internal staff compromise

It is more difficult to prevent internal staff fraud than stopping hackers to compromise the security of an organization. Internal fraud includes salami techniques, where small amounts of money are being taken from big amounts to prevent detection. By applying segregation of duties, job rotation and mandatory vacations, the risk of abuse can be vastly reduced. It is also essential that passwords, computer access controls and user identifications remain confidential to reduce exploitation. Other measures to limit internal staff compromise include background checking for new staff recruitment, regular audits, code of conduct reminder, counselling services, and employing quality staff and remunerate them fairly.

2.7 Inadequate customer education and awareness

Lack of customer education and awareness in terms of safeguarding their online transactions can open holes for hackers who can a false screen for the customer to input confidential information that get sent to the hackers or transfer the money to the hacker's account. Financial institutions must take a note that customer education is of paramount importance. They should ensure that customers are aware that they have a role to play to safeguards their interests because customers may easily overlook some key precautionary principles. Financial institutions should ensure Internet banking security awareness to their customers such as in-housing programs plus community-wide programs.

2.8 Breaches of legislation

Financial institution is governed by some legislation or Acts such as Financial Services Sector Charter and the failure to comply can be very risky to its survival. Regulatory changes may have an impact on the financial institution system and business strategy. Thus, it is very imperative for the financial institution to keep up-to-date and comply with the legislation. It is also advisable to keep close liaison with law enforcement authorities and regulators for best practice sharing/influence.

2.9 Web spoofing

Online criminals often establish so-called "spoof sites": using websites that they have created, using the HTML code of legitimate business websites to make their sites look exactly like the legitimate businesses' sites. By sending emails with false information to the legitimate businesses' customers, these criminals can trick customers into entering larger amounts of valuable personal data and then

use those data to access existing financial accounts or establish new accounts. Enterprises with established Web presences therefore need to maintain some form of proactive surveillance to spot, as soon as possible, whenever someone has set up a spoof site. When a spoof site is found, the enterprise should also contact the pertinent Internet Service Provider to have the offending site taken down and make a prompt referral of the matter to law enforcement.

2.10 PAIN risks

The four main risks of e-business comprise of: Privacy of transactions; Authentication of individuals who have rights to access e-business systems; Integrity of data in transit and in storage; and Non-repudiation of transacted business: PAIN. The countermeasure of PAIN risks is Public key infrastructure (PKI) which ensures authentication, confidentiality, non-repudiation, and message integrity by using both symmetric and asymmetric algorithms and hashing and digital signature algorithms.

3 ANALYSIS OF FINANCIAL INDUSTRY

The analysis of the financial industry is performed using two existing models: industry analysis and competitor analysis (Fleisher and Bensoussan, 2003).

3.1 Industry analysis

Michael Porters' Five Forces model (Fleisher and Bensoussan, 2003) is used, in this study, to analyse major economic and technological forces in the financial services industry that will ultimately influence an industry's profit potential. Identifying these profit potential of the industry provides the foundation for bridging the strategic gap between the firm's external environment and its resources. The five forces are classified as rivalry among existing competitors, threats of new entrants, threat of new substitute products or services, bargaining powers of buyers, and bargaining power of suppliers.

3.1.1 Rivalry among existing competitors

The market for treasury is large; $10bn daily (Jessen, 2001). The banking industry is dominated by the four major banks referred to as the BIG FOUR, namely, ABSA, First Rand, Nedcor, and Standard Bank. The insurance industry is also dominated by the four major companies, namely, Old Mutual, Sanlam, Liberty Life, and Momentum. The number of players in the financial services industry in South Africa is increasing. This increase of players increases rivalry in the treasury services market. The growth in the treasury market is also increasing. The costs are high and many of them are fixed (Jessen, 2001).

3.1.2 Threats of new entrants

The online financial services market is constantly evolving and new entrants to this market are continually emerging. The barriers to entry are not particularly high, even though the experience curve does have some impacts. The likelihood does not seem high, however. International players could also enter and the only real barrier to entry would be if the existing players have market dominance and high quality customer relationships. Most new entrants are focusing on particular segments of a fragmented market. This new entrant has the loyalty advantage of its existing customers, existing value added services such as investment research, and the monetary backing of firms with existing and ongoing revenue streams.

3.1.3 Threat of substitute products or services

The consensus is that the trend is towards outsourcing the treasury, simply because the market is highly volatile and requires specialised skills to deal with the prevailing challenges. Necessary skills that many financial services industries do not always have can often be acquired at great costs.

3.1.4 Bargaining power of buyers

The bargaining power of buyers is currently low due to undifferentiated products/services, but is increasing slowly and sophisticated as buyers are demanding greater choice and better quality service. The buyer propensity to move to a more innovative institution is also increasing. Over time, the buyers will increase to have more power, particularly as foreign exchange becomes more of a commodity and the rivalry among banks for additional volume increases.

3.1.5 Bargaining power of suppliers

Few suppliers have high bargaining power due to the fact that they are pricing the credit risk for dealing with the clients and due to dependence on innovations that are essential to financial services industry's inputs. Over time, the bargaining power will shift towards outsourced companies and web-enabled intermediaries with increasing higher skills levels.

3.2 Competitor analysis

Internet banking has emerged over the recent years with 500,000 out of the 2 million Internet-connected South African customers banking online (Baloyi, 2005). Internet banking of five financial banking institutions (ABSA, Standard Bank, FNB, Nedbank, and Investec) are compared and contrasted in terms of online secure e-business products/services offerings, Table 1. The importance of this table is to identify online secure e-business approaches provided by these institutions. This study utilized public available information. Because of the similarity of the online services, financial insurance institutions are not discussed in this paper, but can be found in Baloyi (2005).

Table 1: Secure e-business products / services of banking institutions

SERVICES	**ABSA**	**STANDARD BANK**	**FNB**	**NEDBANK**	**INVESTEC**
Identification	Users are required to register, choose access account number and PIN	Also uses account number and PIN	User name is used to identify the user	Access number is randomly generated for the customer, while a PIN number is selected by the customer	Uses ID number and PIN that must be different and have a minimum of 5 digits
Authentication	Users select password	Password with preferred specifications is used for logon	Password is used to authenticate the user	Two factor authentication (passwords and smartcards) is used	
Confidentiality	Encryption is built into browsers; SSL	128-bit secure encryption; SSL	128-bit encryption; SSL	128-bit encrypted SSL is used for all connections	128-bit SSL encryption is used
	Uses VeriSign to secure electronic	Certificate is VeriSign Trust	VeriSign process is available on	Digital certificates are	Site certificate issued to verify

SERVICES	ABSA	STANDARD BANK	FNB	NEDBANK	INVESTEC
	transactions of any kind	Network authenticated	the website	used	the sites' genuineness
Technical solutions	Multiple firewalls are used	Protects servers with the use of firewalls		Firewalls and servers checked regularly for vulnerabilities.	Firewalls are used
	Users use same antivirus	Delegate independence use of antivirus package to customers		Independent antivirus is used by customers	
		IDS is deployed to detect intrusions			
Timeout operation	4 minutes	5 minutes		10 minutes	10 minutes
Advice to users		Have informative guidelines to users		Informative guidelines are provided to clients	Provides more guidelines to users

Financial banking institutions offer similar kind of online secure e-business solutions.

4 SECURE E-BUSINESS STRATEGIC SOLUTIONS: PROCESS-ORIENTED APPROACH

Secure e-business solutions cannot be described by a list of security controls, but they require that all components be properly integrated together and run smoothly. Financial industries should look at transforming e-business, covering integration both the front and back office and across communications networks and multiple applications. This section provides processes-oriented (integrated) approach that could be deployed for secure B2B and B2C transactions.

4.1 Pre e-business transactions

Due to the nature of its business, financial institution should conduct pre-employment background check before hiring employees, i.e. background check (including education and references), drug screening, security clearance, and credit check. Employees should be well supervised, warned about industry espionage and be required to sign a nondisclosure agreement. Apply segregation of duties and ensure that the knowledge needed to effect a fraud is compartmentalised. Other important considerations are: disabling all unnecessary communication ports to prevent copying of sensitive data by staff, removal of all dormant or expired IDs and customer accounts, ensuring that activity and security logs are activated and reviewed regularly and ensuring that after office hours transactions are blocked and be particularly vigilant during holiday periods.

4.2 Identification

Users should register and choose username, ID number and personal identification number (PIN). Access account number should be randomly generated for the customer and dynamic to ensure no

duplicates. ID and PIN number must be different and must consist of a minimum of certain digits (e.g. 6) depending on the requirements of the organization.

Random online keypad should be used to help combat identity fraud. This application will ensure that customers protect confidential information as a secure means of entering secure credentials.

Users should also be required to complete once-off number of questions (e.g. 10 out of 15 questions) that will be used to authenticate legitimate user in case he/she forgets PIN or ID number.

4.3 Authentication

Authentication means that access to an e-business system is limited to those who can provide the proper identity credentials. The common use of authentication is through the use of a logon ID and password. Digital security service should be used on top of user ID and password to add another access layer to protect the accounts linked to customers' profile by generating a unique security code each time a user login to the site. Access should be denied after three unsuccessful PIN code / password attempts. In order to reset a PIN, users should contact their branch or use online reset application if they chose this functionality upon resetting up their passwords.

Password authentication is considered a very low level of authentication as it is often easy to break. Organizations should make use of two-factor authentication, i.e. password and smartcard, password and biometric, or smartcard and biometric authentication.

Digital certificate, as the identity credential, is very much secure as a means of authentication and is very advisable for financial institutions. Digital certificates can be stored in the web browser or smartcard. Digital certificates stored in the browser are used to access various sites on the Internet. In the later case, the smart card is inserted into a special reader to access a secured system. The secured system reads the digital certificate stored on the card and decides whether to allow access to the user or not.

If the user is carrying out business from an insecure workstation, the user should be given a token based on a challenge-response protocol using a symmetric algorithm. Alternatively, the user could utilize his/her mobile phone to exchange one-time password, thus providing a separate secure channel to the backend for authorization of his/her signature. The proposal here is to use the token to authorize the generation of a signature, not to authorize a transaction.

4.4 Authorization

After authentication into the systems, there should be authorization of processing whatever applications a user (employee) or customer has been assigned responsibilities to. In this respect, the principles of least privileges, need-to-know and database views are applied to ensure that proper authorization is effective for any e-business transaction.

4.5 Creation and stoppage of third-party payment

Financial institution should allow customers to make use of unique random reference (verification) number to control the creation of valid beneficiary to their profiles and stop payment. Future dated payment functionality is also provided by this application. Short message service (SMS) functionality via cellphones or email is received by users to authenticate the client and authorize a third-party payment.

4.6 Network security systems

Financial institution must ensure front-end and back-end network security services for all e-business transactions to be more secure. This will mean installing virus prevention and detection

systems, firewalls and intrusion prevention and detection systems. Periodic security reviews on these systems must be conducted by both internal and external professional security auditors to identify and close up vulnerabilities.

4.7 Secure communications

There are technologies that provide secure communications of B2C and B2B. Financial institutions must deploy security technologies that meet their e-business requirements. This section discusses SSL/TLS/WTLS, secure email, extranet, EFT, VPN, dedicated links, and PKI.

4.7.1 SSL/TLS/WTLS

Secure socket layer (SSL), Transport Layer Security (TLS) protocol, and Wireless Transport Layer Security (WTLS) have been developed for secure Web channel between the client and the bank. This means that the data that is transmitted between both ends is kept secret (confidential) and that tampering will be detected (data integrity); the bank is always authenticated; the client can be required to authenticate too. There are differences between these protocols, but they conceptually provide the same security service. Their detailed information can be found in Rescorla (2000).

4.7.2 Secure Email

Electronic mail (Email) may be the most heavily used feature of the Internet or LANs in an organization. Because of its extensive use, email has become more of a target by attackers, so standards and protocols have been put in place to provide interoperability and better services levels for messages as they get passed back and forth. Secure email allows users to secure their email messages and attachments by adding cryptographic security services, namely Pretty Good Protocol (PGP), Message Security Protocol (MSP), Privacy-Enhanced Mail (PEM), and Secure Multipurpose Internet Mail Extensions (S/MIME). Their cryptographic services include confidentiality, authenticity, non-repudiation and integrity. Digital signatures and return-receipts are some of the services that are provided by the secure email for business-to-consumer transactions.

4.7.3 Extranets

An extranet extends outside the bounds of the company to allow two or more companies to share common information and resources. Extranets are set up by business partners to allow for business-to-business communications to take place.

4.7.4 Electronic fund transfer

Electronic fund transfer (EFT) is the exchange of money via telecommunications without currency actually changing hands. With the use of EFT, sum of money are transferred from one account to another electronically. Security in an EFT environment is extremely important because of the potential high volume of money being exchanged, thus posing high risk. Security includes access security, authorization of processing and data encryption through communications networks.

4.7.5 Virtual private networks

Virtual private network (VPN) is a popular technology that companies use to provide secure communications tunnels through untrusted networks. The connection is made private and secure by encryption and tunnelling protocols.

4.7.6 Dedicated links

Financial institutions can establish permanent connection for business-to-business. Dedicated links offer tremendous security, reliability, and quality of service, but they are extremely expensive and provide no flexibility in connecting with other parties.

4.7.7 Public key infrastructure

Electronic commerce is unthinkable without the involvement of the Public Key Infrastructure (PKI). Elements of the PKI technology provide solutions to the risks of e-business as they can be used to solve each of the risks individually, or PKI technology as a whole can be used as a complete security solution for e-business applications.

PKI uses encryption to ensure that transactions are kept private, thus providing privacy measures from the outside party. PKI technology can use encryption to protect the privacy of data in transit and in storage. With the use of digital certificates, PKI solves the problems associated with the passwords. Digital certificate contains the public key together with personal identification information of the participant in a PKI. PKI uses a technology called "message digest" or "hashing" to ensure data integrity. The message digest is a common way of verifying data integrity in transmission. Non-repudiation is commonly provided by digital signatures. The solutions to privacy, authentication, integrity and non-repudiation (PAIN) risks are all provided by the PKI.

4.8 Inactivity time-period

Timeout operation should be applied if users log on into the system and don't use the service for certain period of time. To access the accounts again, users have to logon again.

4.9 Secure back-end

Secure backend, a way forward which is flexible, mobile, and secure, should be made available for each user, providing a virtual smartcard. This secure backend is a fast tamper resistant hardware unit, which may service a number of users at the same time with each having an individual key pair (Landrock, 2003). Each user has secure access to a unique key pair in the unit by means of a secure token. The user is also responsible for his/her own key generation.

4.10 Post e-business transactions

Transactions notifications should be used by financial institution to notify users immediately of transactions conducted on their accounts and any logins to their profiles. This innovative messaging service helps users track any transactions and also provides confidence and peace of mind.

It is also necessary for the financial institution to provide confidence to the online users. The presence of WebTrust sign on the website can inform potential customers that the website has been evaluated and meet criteria such as business practices disclosure, transaction integrity, and information protection. Guarantees to reimburse users for any losses due to fraud via its website can be another way for the financial institution to provide confidence to the users in terms of its security systems' robustness and encourage more customers to go online.

4.11 Secure information storage

Financial institutions must be committed to keep customer information secure and confidential. Personal information collected via the Website should be stored in a secure environment and not be available to any person outside the organization. Smartcards may be used to securely lock the digital certificates in a secure, removable medium, making them inaccessible to anyone but their rightful owner.

5 FUTURE RESEARCH

Financial services industry is experiencing a number of web-enabled brokerages and exchanges, which is positive. Online trading volumes are growing, driving down trading revenues (Jessen,

2001). Telephone banking is more likely to be the next major development as the number of cellular phone users is increasing significantly. The major reason for this development is because users are demanding very flexible solutions, which allow them to carry out their business from virtually anywhere in the world.

The role of information security in an electronic business environment has changed as it no longer exists only to protect against risks but also as a part of the quality of service offered. There are some elements that must be taken into consideration when creating a secure system. Like all good business solutions, the first element of any business planned change must derive from the formulation of strategy. E-business must be carried out in the context of strategy. Financial institutions should look at the high level strategic issues which they need to consider in answering the question of where they want their business to be in five years.

- **Intensity of the competition**: Electronic distribution will benefit some financial services providers significantly from the potential for reach and product diversification. Some financial services providers will become niche players as they retreat to a cost effective core product. Online services will include banking, brokerage, life and other retail insurance, retirement and estate planning, funds provision, mortgages, credit cards, and much more. The winning providers may ultimately be those which can provide a one-stop service and which can draw on their customers database more efficiently and effectively to support cross-selling.

- **First mover advantage:** There will be an edge from being first into a market which can translate into more captive clients, improved economies of scale, better brand development and potentially greater margins.

- **Confidence of new entrants:** The Web has fast forwarded the time to market for new products. There are many new players in the market with bold ideas and aggressive execution which will drive down margins for the industry by: improving pricing transparency and empowering the consumer with education and information, instant access to products, and attacking inefficient links in the distribution chain. Comparison shopping and auction-style marketplaces will grow in popularity among consumers.

- **Discerning by consumers:** Technology is shifting the balance of power from traditional financial services providers towards the end-user, for both corporate and retail customers. The ease of information on the Internet will ultimately create more discerning buyers as people find it easier to do their own price and value comparisons of products or services. Therefore, it is very important for product-driven financial services providers to transform themselves into market-driven and customer-focused companies.

- **Distribution channels consideration:** E-business channels may add new business, but will also challenge existing relationships.

- **The impact of price transparency:** The pricing information on the Internet is readily available to enable consumers to shop at home for the best prices. This pricing information together with increased competition will likely reduce costs to online consumers for some financial products over the next few years.

- **Cost reduction to match revenue generation:** The use of e-business to reduce cost is essential to competitive success. Margin reductions will be balanced with cost-cutting opportunities.

- **Customer loyalty retention:** Financial services providers will need to be prepared to counter the pricing pressure that will result from e-business competition, for example, increasing commoditisation through pricing innovation and customisation, focus on responsive and

dedicated services, market programs to create direct electronic customer relationships and avoid over-reliance on intermediaries for new business.

6 CONCLUSIONS

Financial institutions are recognizing that criminals can pose a broader and more sophisticated variety threats to valuable corporate assets – principal information assets – through the use of computing tools and Internet access. The safety of online banking is dependent on the security systems of the financial institutions and the precautions customers take to safeguard their User ID and PIN, as well as protecting the PCs they use. For example, customers should install firewalls, intrusion detection systems and anti-virus software on their PCs to block out hackers and log off their computers when not in use.

Managers should therefore factor human vulnerabilities into Internet fraud risk calculus, and budget for thorough training, creative prevention and education messaging tailored to the needs of their enterprises, and where necessary build in technological measures to minimize the risks to information assets that momentary misjudgements could trigger. Financial institutions therefore need to begin reorienting their thinking about Internet fraud and how it can affect their individual enterprises and customers. They must engage themselves actively on security technology trends and continuously educate, update and precaution their customers on latest fraud or security countermeasures; knowing that what is secure today may not be secure tomorrow.

7 REFERENCES

Bequai, A. (1998). "Employee abuses in cyberspace: Management's legal quagmire". Computers & Security, Vol. 17, pp. 667-670.

Baloyi, N.T. (2005). "Strategic secure enablement of the business of e-Business in the financial institution". Unpublished research report submitted in partial fulfilment of the requirements for the MBA dissertation. University of Kwazulu-Natal, Durban, South Africa.

Deloitte & Touché. 2002. E-business in the financial institution, white paper, www.deloitte.com/dtt/cda/doc/content/ebus.pdf.

Fleisher, C.S. and Bensoussan, B.E. (2003). Strategic and Competitive Analysis: Methods and Techniques for Analysing Business Competition. Pearson Education, Inc., New Jersey.

Granova, A. and Eloff, J.H.P. (2004). "Online banking and identity theft: who carries the risk?" Computer Fraud & Security, November, pp. 7-11.

Jessen, M. (2001). "An assessment on the web-enabled intermediaries' impact on the financial institutions in the treasury services market: an industry analysis of the financial services within South Africa". Unpublished research report submitted in partial fulfilment of the requirements for the MBA dissertation. Gordon Institute of Business Science, University of Pretoria, South Africa.

Landrock, P. (2003). "Electronic commerce – how to get the security right?" Computer Fraud & Security, June, pp. 6-9.

Lichtenstein, S. (2000). "Internet risks for companies". Computers & Security, Vol. 17, pp.143-150.

Philippsohn, S. and Thomas, S. (2003). "E-Fraud – what companies face today". Computer Fraud & Security". January, pp. 7-8.