System Security & Fraud Concerns: ICT Interventions in the Banking Sector

Isaac Awuondo
Managing Director
Commercial Bank of Africa Limited.

Contents

- About CBA
  - Brief History of CBA
  - CBA's Target Customers
  - Financial Performance of CBA
- System Security & Fraud Concerns: ICT Interventions in the Banking Sector
  - Financial Insights Opinion
  - Situation Overview
  - Strategies for Managing Security in a 24/7 World
  - Future Trends and Direction

Brief History of CBA:

- Founded in 1962, CBA commenced operations in Dar-es-Salaam, Tanzania.
- Thereafter established branches in Kenya and Uganda
- CBA was re-incorporated in Kenya in 1967 after operations were nationalised in Tanzania.
- CBA originally commenced business as a subsidiary of Societe Financiere pour les pays D'Outre Mer (SFOM), a Swiss-based consortium bank with interests in financial institutions throughout Africa. Initial shareholders were:
  - Bank of America, Commerzbank AG, Banque Bruxelles Lambert and Banque Nationale de Paris
- In 1980, Bank of America acquired all the shares of the other SFOM partners making CBA a wholly owned subsidiary of Bank of America with 16% of the shares held by Kenyan investors. In 1991, Kenyan investors acquired total shareholding and CBA became wholly Kenyan owned and managed
- In 2005, acquired First American Bank of Kenya (FABK), and became the largest privately owned local bank in Kenya. This acquisition also marked the re-entry of CBA into the Tanzania with a 20% equity stake in UBA. The majority stake in UBA was acquired in 2007 to make this a subsidiary
- CBA acquired a 33.3% equity stake in AIG Kenya Ltd in 2006
- In 2006, CBA relocated to new ultra modern head office premises in Upper Hill

CBA's Target Customers

Corporate Customers

- Multinational and medium-to-large Kenyan corporate
- Diplomatic missions and related development organisations
- International organisations and agencies
- Non-Governmental Organisations

Personal Customers

- Employees of the above organisations
- Medium-to-High Net Worth individuals

Financial Performance of CBA

- Growth resulting from focused business model backed by service quality and operating efficiency:
  - Pre-tax profits have risen from KShs 70 million in 1991 to KShs 1.376 billion as at 31st Dec 2006 (audited)
  - Total assets have increased from KShs 2.2 billion to more than KShs 37.4 billion as at 31st Dec 2006 (audited)
  - Shareholders funds have increased from KShs 240 million to KShs 3.72 billion during the same period

System Security & Fraud Concerns: ICT Interventions in the Banking Sector

Financial Insights Opinion

- **Security attacks against financial institutions and their customers are growing and are increasingly connected with consumer and corporate fraud schemes**
- Managing data security in today's distributed technology environment is much more complex because the function must go beyond an institution's boundaries to control security risks facing service providers, remote partners, and customers
- Financial institutions are currently adapting security risk management to the new environment in the following ways:
  - ∞ Investing in security management tools that enable more proactive management of security;
  - ∞ Increasing the formality, frequency, and business relevance of security risk assessments; or
  - ∞ Outsourcing the most time-consuming security management functions to security services providers.

Financial Insights Opinion

- **New technologies and strategies being contemplated to manage internal and external consumer security risk today include:**
  - Collaborating with technology providers - both security specific and financial services specific - to develop new solutions to help customers prevent fraud schemes perpetrated through email and Web technology (such as phishing); and
  - Evaluating more secure authentication solutions for customers transacting in an online environment and employees using the internet to offer transaction support.

Situation Overview

The importance of information security (IS) in the banking industry has grown tremendously over the last few years due to a combination of factors including but not limited to:

- **Growing severity and number of security attacks** in the form of email fraud, viruses, worms, and other malicious code against financial institutions and their customers
- **Increased exposure to risk of data theft, destruction, or manipulation from insiders** due to the greater availability of information in electronic format and the increased mobility and access of information via networked computers spanning the enterprise and the globe

Situation Overview

Financial organisations must accomplish the following objectives:

- ***Availability*** - the processes, policies, and controls used to ensure authorised users have prompt access to transaction information
- ***Integrity of Data or Systems*** - the processes, policies, and controls used to ensure information has not been altered in an unauthorised manner and that systems are free from unauthorised manipulation that will compromise accuracy, completeness and reliability
- ***Confidentiality of Data or Systems*** - the processes, policies, and controls employed to protect information of customers and the institution against unauthorised access or use
- ***Accountability*** - the processes, policies, and controls necessary to trace actions to their source
- ***Assurance*** - the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended

Situation Overview

Financial institutions must protect their information by instituting a security process that:

- Identifies risks
- Develops a strategy to manage the risks
- Implements the strategy
- Tests the implementation
- Monitors the environment to control the risks

Situation Overview

- ***The following 5 areas serve as a framework and outline the method an organisation should use to implement and achieve its security objectives:***
  - *Information Security Strategy*
  - *Information Security Risk Assessment*
  - *Security Controls Implementation*
  - *Security Monitoring*
  - *Security Process Monitoring & Updating*

Strategies for Managing Security in a 24/7 World

- **Security Management Becoming More Proactive**
  - ∞ In response to these security threats and requirements, banks and their service providers have been investing in security management tools that enable a more proactive management of security
  - ∞ Investments in security detection and incident response remain strong; however, given the nature of security, there will always be a hacker or criminal out there identifying some vulnerability somewhere
  - ∞ Providers of security detection solutions are starting to offer proactive solutions that can start preventing attacks after detecting them

Strategies for Managing Security in a 24/7 World

- **Demands of Security Management Driving Outsourcing**
  - ∞ While the increasing number of security attacks has led many financial institutions to increase their investments in tools and personnel for the day-to-day management of security, these challenges have led several institutions to outsource all or a portion of security management to third-party service providers
  - ∞ A significant driver of these outsourcing deals is access to security intelligence. Providers of security services have access to comprehensive internet security information because they monitor security events across firms around the world

Strategies for Managing Security in a 24/7 World

- **Expanding Data Security Boundaries**
- ***Service Provider Security***
  - ∞ The expanding geographic boundaries of a financial institution's business create new security risks. A key risk management priority for financial institutions today is ensuring that the service providers have adequate security controls to detect and prevent breaches in the confidentiality and integrity of customer information
  - ∞ However, the industry is realising that security reviews and detailed service-level agreements (SLAs) that include security and fraud risk assessment and control may not be enough to mitigate security and fraud risks
  - ∞ Financial institutions need better tools to assess security risks faced by third-party vendors in order to make more informed decisions about their service providers and to better manage the partner relationship

Strategies for Managing Security in a 24/7 World

- **Expanding Data Security Boundaries**
- ***Service Provider Security***
  - ∞ Management of information security in the customer's area of control is a new challenge that institutions have only started to tackle. Institutions are still grappling with how to prevent the loss of trust in an environment in which customers are constantly receiving emails from fraudsters asking them to reveal confidential information - The famous 411 Fraud
  - ∞ On the other hand, criminals are developing new ways of stealing consumer data to perpetrate fraud, yet the industry is still using old defenses. The practice of requiring usernames and passwords as the sole means for online authentication is rapidly becoming outdated
  - ∞ Fortunately, stronger authentication technology is an effective weapon to combat the rising tide of consumer data theft. Stronger authentication offers additional means to validate users even if the customer's logon credentials are compromised

Future Trends and Directions

Technology is developing very quickly. The following sections discuss briefly the security issues which are helping to shape the security directions likely to be taken by many of the banks

Future Trends and Directions

- **Non-Repudiation**
  - The continual expansion of private banking networks has started a trend where the banks have to relinquish a degree of control to the security of customer or retailer computer interfaces. The absence of manual ability to sign transactions will continue to become a difficult issue. There is a business need for a trust in the business trading relationships between the two parties, as well as defined contractual responsibilities
  - Some banking systems have already implemented digital signature security schemes, but other banks are more likely to introduce such measures with the newer EDI developments within the corporate banking sectors

Future Trends and Directions

- **Smart Disks**
  - Other types of technology such as "smart disks" (disks with built-in microprocessor) are likely to find a market niche, not only within banks but also in more general PC security solutions

Future Trends and Directions

- **Security Architectures for Cryptographic Services**
  - The costs of designing and implementing central cryptographic architectures has until now mainly been met by individual system developments
  - These developments are typically based upon a central security server, which can be used in a flexible fashion to provide the full range of security services

Future Trends and Directions

- **Contactless Cards and DSV Techniques**
  - ∞ The use of Dynamic Signature Verification (DSV) schemes has many benefits in terms of customer acceptability
  - ∞ Mass exploitation of smart cards will require an extremely durable token which can sustain a long life span

Future Trends and Directions

- **Integrated Service Digital Network**
  - ∞ Known by the acronym ISDN, this technology is now poised to revolutionise communications, and can be used to support the transmission of voice, data, image or even television
  - ∞ There is little doubt that ISDN will pave the way in the security field for speeding up and introducing new methods of remote user verification. However, the development of both national and global standards may well hamper the process in the short term

Future Trends and Directions

- **Stronger Authentication Solutions**
- ***Internal Use***
  - ∞ While access control projects have been at the forefront, authentication projects have been less so. Employees continue to use single-factor authentication methods, namely login name and password, to access applications
  - ∞ Several institutions are using smart cards to manage physical security and voice authentication to allow employees to reset their passwords via phone, a technology which has not been replicated locally

Future Trends and Directions

- **Stronger Authentication Solutions**
- ***Online Customer Services***
  - ∞ Multifactor authentication solutions for customer adoption are back on the drawing board. Financial institutions have held the belief that solutions requiring customers to perform an additional task, such as purchasing a hardware device or downloading software, were doomed for failure
  - ∞ Several options being considered today involve the use of an image or picture chosen by the customer as a means of authenticating the Web site or the customer
  - ∞ The industry will have to be wary of enrolling their customers in these security programs via email campaigns given that recent phishing schemes have been targeting these security services
  - ∞ Other authentication solutions being considered require less effort on the part of customers

Future Trends and Directions

- **Proactive Online Fraud Management**
  - ∞ Financial institutions are starting to join forces with technology providers in all sectors to identify ways to make the internet a safer place for consumers
  - ∞ Managed security services typically include vulnerability monitoring and security event detection / prevention and response

Future Trends and Directions

- **Proactive Online Fraud Management**
  - ∞ **The capabilities and expertise financial institutions seek from providers of security technology have expanded beyond those aimed at implementing in-house security technologies**
  - ∞ **A wider range of institutions are seeking to outsource security management to managed security services providers**
  - ∞ **Institutions are seeking security information management and risk assessment tools to improve security risk management**
  - ∞ **Institutions are looking for more powerful security event analytics that can detect fraud schemes such as phishing or fraud perpetrated via the online banking channel**

Future Trends and Directions

- ***Essential Guidance***
  - ∞ ***The severity of security attacks launched against financial institutions and their customers continues to grow as criminals, hackers, and fraudsters take advantage of gaps in internet technology and in-house security to organise increasingly damaging attacks***
  - ∞ ***Financial institutions today are forced to adopt a more proactive approach towards security risk management as they try to stay one step ahead of their attacks by patching vulnerabilities before they can be exploited***

Future Trends and Directions

- ***Essential Guidance***
  - ∞ New technologies and strategies being contemplated to manage internal and external consumer security risk today include the following:
    - ∞ ***Collaboration with technology providers- both security and financial services specific - to develop new solutions to help customers prevent fraud schemes perpetrated through email and Web technology (namely phishing); and***
    - ∞ ***Evaluation of more secure authentication solutions for internal employee authentication and, in some cases, for authentication of customers and institutions in the online environment***
  - ∞ These enhancements and approaches show that financial institutions are evolving their management of internal security to tackle the new security threats of today. However, their approach to the management of security risks on the service provider side and on the customer side remains timid