Security and Privacy of Electronic Banking

Zachary B. Omariba

PhD. Candidate, Masinde Muliro University of Science and Technology

Nelson B. Masese

PhD. Candidate, Masinde Muliro University of Science and Technology

Dr. G. Wanyembi

Senior Lecturer, *Masinde Muliro University of Science and Technology*

Abstract:

The internet has played a key role in changing how we interact with other people and how we do business today. As a result of the internet, electronic commerce has emerged, allowing business to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The e-banking system addresses several emerging trends: customer's demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are concerns of security and privacy of information. This paper will first discuss the drivers of e-banking; secondly, it will talk about the concerns about e-banking from various perspectives. Thirdly, the security and privacy issues will also be discussed, and fourthly the attacks of e-banking with their solutions are discussed.

Keywords: *Internet, e-commerce, e-banking, security, privacy, and attacks.*

Introduction

The information superhighway has found its way into many homes, schools, businesses, and institutions. Many people are cruising the internet each day to obtain information on the weather, latest sport scores, job offers, local news, and may other exciting information. These people also buy and sell goods on this media. Consequently many businesses are reaching out to customers worldwide using the internet as its communication channel. This new electronic media of interaction has grown to be known as electronic commerce (E-commerce). E-commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information. Also e-commerce is comprised of interconnected communications networks; advanced computer hardware and software tools and services; established business transaction, data exchange, and interoperability standards; accepted security and privacy provisions; and suitable managerial and cultural practices. This infrastructure facilitates diverse and distributed companies nationwide to rapidly, flexibly, and securely exchange information to drive their business processes.

The banking industries are one such business that is using this new communication media to offer its customers value added service and convenience. This system of interaction between the consumers and the banking industries is called the electronic banking system. FinCen (2000) states that “E-banking is an umbrella term for the process by which customer may perform banking transactions electronically without visiting a brick-and-mortar institution”. E-banking is the use of electronic means to deliver banking services, mainly through the internet. The term is also used to refer to ATMs, telephone banking, use of plastic money, mobile phone banking, and electronic funds transfers.

E-banking is the use of a computer to retrieve and process banking data (statements, transactions details, etc) and to initiate transactions (payments, transfers, requests for services, etc) directly with a bank or other financial services provider remotely via telecommunications network. Electronic banking system addresses several emerging trends: customer demand for anytime, anywhere service, product-to-market imperatives and increasingly complex back-office integration challenges. This system allows consumers to access their banking accounts, review most recent transactions, request a current statement, view current product information, and re-order checks. Some of the banks that are currently offering this service in Kenya are Standard Chartered Bank, Kenya Commercial Bank, Barclays Bank of Kenya, Equity bank, Consolidated Bank of Kenya, Commercial bank of Africa, Cooperative bank of Kenya, National Bank, Family Bank, among others.

The e-banking system can be seen as an extension of existing banks. These banks are catering to a very large population of internet users. Heidi Goff, Senior Vice President for Global Point of Interaction of MasterCard estimated that there will be more than 100 million users by the year 2000. This projection was right as the number of internet users rose to 361 million people globally, which was a 5.8% of world population in the year 2000. According to the internet world statistics, internet users stood at 2,267 million which is actually 32.7% of the world population in December 2011. Many other estimates conclude similar results, which lead to the indication that the internet will play a major role in everyone’s life and promote the electronic banking industry.

The current focus of security of information transfer is on the session layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over un trusted channels and a trusted code at both endpoints. The solution addresses the use of secure protocols because trusted channels don’t really exist in most of the environment especially since we are dealing with linking to the consumers. The solutions of the security issues require the use of software- based systems or hardware-based systems or a hybrid of the two. These software-based solutions involve the use of encryption algorithms, private and public keys, and digital signatures and pretty good privacy. Hardware-based solutions such as the Smartcard and the MeChip provide better protection for the confidentiality of personal information. Software-based solutions have advantage over hardware-based solutions in that they are easy to distribute and are generally less expensive.

Drivers of Electronic Banking

As internet continues to expand, the convenience associated with electronic banking will attract more customers. One expectation of e-banking is that it will replace the need for writing checks, or carrying a lot of cash. In today's market, "according to the preliminary data from the latest Federal Reserve survey of patterns of consumer spending, almost four-fifths of consumer expenditures are handled by checks, directly or indirectly. According to Consumer Federation of Kenya (COFEK), mobile phones now drive Kenya's consumer spending. *Kenyan consumers are increasingly turning to social media and mobile phone advertising to guide their spending.*

A survey of Kenyans' digital habits by research firm TNS RMS East Africa found that 73 per cent of Kenyans would be happy doing their entire Internet surfing on their phones. Further, 67 per cent use social media to research brands, and around half of them would like to be able to purchase products through social networks. "Growth in Internet access offers big opportunities for brands and marketers that can be explored with the right strategies," said the TNS associate director of technology, Mr. Bob Bugoyne.

A report by the Central Bank of Kenya shows that the number of mobile money users in Kenya increased to 19.2 million in 2011, with 15.21 million of them being M-PESA customers. Whereas P2P (person-2-person) transactions are still dominant, the report shows that business to persons and persons to business transactions are increasing. In the month of December 2011 alone, the amount transacted between individuals and businesses stood at sh54.53 Billion, which translates to roughly 46 per cent of total amount transacted that month. In that month, M-PESA moved sh116.6 Billion.

This means that electronic banking has a very large potential for use since many people expect that electronic checks will substitute paper checks. For consumers, electronic money means greater efficiency that using coins, notes, and traditional banks. The e-banking system brings the convenience of 24-hour, seven days a week, banking by offering home PCs tied directly to s bank's computers. In addition, electronic money also offers greater security than paper-and-coin system.

The increasing application of advanced technological solutions in banking operations has transformed the country's financial sector, and opened up avenues of reaching out to the unbanked population. Citibank Group has lauded the success of Kenya's electronic commerce, and urged other economies in sub-Saharan Africa to replicate the Kenyan model. The US-based financial conglomerate notes that Kenya's e-commerce presents an operationally efficient and cost-effective payment and collection solution to the unbanked population.

In a report dubbed: 'Financial Trends of the Development Sector in Kenya and Africa', the bank observes that with the expansion of electronic commerce, companies are now looking to streamline their processes — without compromising security, confidentiality, compliance, auditability and integrity of transactions. According to the Global System for Mobile Communications Association (GSMA), about 40 per cent of Africa's one billion population has mobile phones, but only 20 per cent have bank accounts. Citibank also pointed out that Kenya was one of the largest recipients of aid in Africa, with a total of $1.8 trillion (Sh165.6 trillion) worth of Official Development Assistance (ODA) received in 2009.

But the bank raised concern that securely managing the receipt and distribution of donor aid flows within Kenya's complex — and often paper-based market — creates many challenges. Kenya's banking industry has witnessed tremendous changes linked with the developments in Information Communication Technology (ICT) over the years. The quest for survival, global relevance, maintenance of existing market share and sustainable development has made exploitation of ICT imperative in the industry. Application of ICT concepts, techniques and the development of policies and strategies has become a subject of fundamental importance and concern to all banks, and is a prerequisite for local and global competitiveness.

Concerns about Electronic Banking

Since e-banking is a new technology that has many capabilities and also many potential, users are hesitant to use the system. The use of e-banking has brought many concerns from different perspectives: government, business, banks, individuals and technology.

Government

From a government point of view, the electronic banking system poses a threat to the antitrust laws. Electronic banking also arouse concerns about the reserve requirements of banks deposit insurance and the consumer protection laws associated with electronic transfer of money. On the other hand, this has not been readily accepted by its users due to the concerns raised by various groups, especially in the areas of security and privacy. Moreover there are many potential problems associated with this industry due to imperfection of the security methods. The example of Postal Corporations Posta pay led to more concerns about this system. This came as efforts by the Postal Corporation of Kenya to embrace technology hit a snag, with the government sending forensic auditors to probe the integrity of its electronic money transfer service, Posta pay, following reports of millions of shillings lost to fraudsters.

At the center of controversy was an agreement between the Postal Corporation and Afripayments, which allows the public to send money using Posta pay and withdraw funds from any post office. The partnership, as crafted, had left the software supplier with undue control over Posta pay operations, exposing the Postal Corporation to heavy revenue losses, said Bitange Ndemo, permanent secretary in the Kenyan Ministry of Information and Communications.

The agreement stipulates that the Postal Corporation is entitled to 20 percent of profits, while Afripayments receives 80 percent. Posta pay was launched in 2006 and has since been exposed to fraudsters. Gaining access to the electronic money transfer system, these fraudsters make it appear as if money has been sent when it has not been, enabling them to withdraw funds and causing losses to the corporation.

The government wants the forensic auditors to determine why the volume of business handled by Posta pay has decreased from 600 million Kenyan shillings (US$8.6 million) per month in 2006 to 400 million shillings in 2007. The auditors were also expected to establish ways in which the agreement is compromising accountability and transparency in the state-owned Postal Corporation.

In order to reduce the potential vulnerabilities regarding to the security, many vendors have developed various solutions in both software-based and hardware-based systems. However software-based solutions are more common because they are easier to distribute and are less expensive. In order for e-banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous.

Businesses

Businesses also raise concerns about this new media of interaction. Since most large transfer of money are done by businesses, there businesses are concerned about the security of their money, while considering the potential savings in time and financial charges associated with this system. Another business concern is connected to the customer. Businesses ponder the thought that there are enough potential customers who would not make a purchase because the business did not offer a particular payment system e.g. electronic cash, electronic check, mobile money (M-pesa). This would result in a loss of sales. On the other side of the coin, if this system becomes wide spread, this would allow more buying power to the customer which puts pressure on businesses to allow consumers to use electronic transfer money.

However, in terms of information security behavior within organizations, security behavior can be seen as part of the organizational culture and may define how employees see the organization. Similarly, organizational culture is a system of learned behavior, which is reflected on the level of end-user awareness and can have an effect on the success or failure of the information security process. Albrechtsen (2007) observes that users considered a user-involving approach to be much more effective for influencing user awareness and behavior in information security. Leach (2003) studied influences that affect a user's security behavior and suggested that by strengthening security culture organizations may have significant security gains. Debar and Viinikka (2006) investigated security information management as an outsourced service and suggested augmenting security procedures as a solution.

Banks

Banks are pressured from other financial institutions to provide a wide range of financial services to their customers. Banks also profit from handling financial transactions, both by charging fees to one or more participants in a transaction and by investing the funds they hold between the time of deposit and the time of withdrawal, also known as the “spread”. With more financial transactions being processed by their central computer systems, banks are also concerned about the security of the system, in particular with the unwarranted access to their accounts. In addition, individuals are also concerned with the secrecy of their personal information. A big percentage of Kenyans poled expressed concern over privacy of computerized data. As more people are exposed to the information superhighway, privacy of information and the security that goes hand and hand with this information is crucial to the growth of electronic transactions.

To add further convenience to the customers, many banking institutions are working together to form an integrated system such as Deposit Protection Fund Board (DPFB), Kenyan Bankers Association, and Kenya Credit Providers Association. In addition, the Association in collaboration with Central Bank of Kenya established the Kenya Credit Information Sharing Initiative (KCISI) in August 2009. This unit operates under the ambit of the Association to coordinate the efforts of members to share credit information through Credit Reference Bureaus licensed by the Central Bank. Formal exchange of credit data among banks commenced with effect from August 2010. Through this initiative, the Association hopes to ensure that lenders make use of vital information on their debtors to differentiate between low and high risk borrowers. This will enhance credit risk management and eventually lead to granting of more favorable terms to low risk customers.

Individuals and Technology:

In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved. The key areas are:

1. Security
   Security of the transactions is the primary concern of the internet-based industries. The lack of security may result in serious damages such as Posta Pay frauds. This section will be discussed in the next section.
2. Anonymity (Privacy)

   By strengthening the privacy technology, this will ensure the secrecy of sender’s personal information and further enhance the security of the transactions. The examples of the private information relating to the banking industry are: the amount of the transaction, the date and time of the transaction, and the name of the merchant where the transaction is taking place. This section will be discussed in the next section.

3. Authentication

Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction. There are two possible ways to verify the integrity of the message. One form of verification is the secure Hash algorithm which is "a check that protects data against most modification". (Pfleeger et al. 1997). The sender transmits the Hash algorithm generated data. The recipient performs the same calculation and compares the two to make sure everything arrived correctly. If the two results are different, a change has occurred in the message.

The other form of verification is through a third party called Certification Authority (CA) with the trust of both the sender and receiver to verify that the electronic currency or the digital signature that they received is real.

4. Divisibility

Electronic money may be divisible into different units of currency, similar to real money. For example, electronic money needs to account for pennies and nickels.

Privacy and Security Issues

Privacy can be understood as a legal concept and as the right to be let alone (S. Warren, et al 1890). Privacy can also mean "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (A.F.Westin, 1967). From a privacy standpoint, trust can be viewed as the customer's expectation that an online business will treat the customer's information fairly (V. Shankar et al, 2002).

There are four basic categories of privacy: information privacy, bodily privacy, communications privacy, and territorial privacy (S. Davies, 1996). Internet privacy is mostly information privacy. Information privacy means the ability of the individual to control information about one's self. Invasions of privacy occur when individuals cannot maintain a substantial degree of control over their personal information and its use.

People react differently to privacy problems. One reason for these differences might be a cultural viewpoint. For example, researchers have pointed out that consumers in Germany react differently to marketing practices than people in the USA might consider the norm (T.Singh et al, 2003). It is also important to understand their views regarding privacy in general, their personal expertise in Internet technologies, and how they view the role of the government and the role of companies in protecting consumer privacy. An individual's perceptions of such external conditions will also vary with personal characteristics and past experiences (N. K. Malhotra et al, 2004). Therefore, consumers often have different opinions about what is fair and what is not fair in collecting and using personal information.

According to C.M.K.Cheung et al (2006) different threats in e-commerce, like data transaction attacks and misuse of financial and personal information, generate security threats. Thus, security is protection against such threats (F. Belanger et al 2002).

Information security consists of three main parts: confidentiality, integrity, and availability. CIA as an abbreviation is a widely used benchmark for evaluation of information system security also

in the e-commerce environment (Parker et al, 2004). All three parts of security may be affected by purely technical issues, natural phenomena, or accidental or deliberate human causes.
Confidentiality refers to limitations of information access and disclosure to authorized users and preventing access by or disclosure to unauthorized users. In other words, confidentiality is an assurance that information is shared only among authorized persons or organizations. Authentication methods, like user IDs and passwords that identify users can help to reach the goal of confidentiality. Other control methods support confidentiality, such as limiting each identified user's access to the data system's resources. Additionally, critical to confidentiality (also to integrity and availability) are protection against malware, spyware, spam and other attacks.

Confidentiality is related to the broader concept of information privacy: limiting access to individuals' personal information. The concept of *integrity* relates to the trustworthiness of information resources. It is used to ensure that information is sufficiently accurate for its purposes. The information should be authentic and complete. For example, forwarding copies of sensitive e-mail threatens both the confidentiality and integrity of the information. *Availability* refers to the availability of information resources. The system is responsible for delivering, processing, and storing information that is accessible when needed, by those who need it. An information system that is not available when you need it is at least as bad as no system at all. It may be much worse if the system is the only way to take care of a certain matter.

As the society and its economic patterns have evolved from the heavy-industrial era to that of information, in terms of providing new products and services to satisfy people's needs, organizational strategies have changed too. In effect, corporations have altered their organizational and managerial structures, as well as work patterns, in order to leverage technology to its greatest advantage such as e-banking services. Economic and technology phenomena such as downsizing, outsourcing, distributed architecture, client/server and e-banking, all include the goal of making organizations leaner and more efficient. However, information systems (IS) are deeply exposed to security threats as organizations push their technological resources to the limit in order to meet organizational needs (Dhillon, 2001; Dhillon and Torkzadeh, 2006).

According to Dr. David Chaum, CEO of DigiCash said that “security is simply the protection of interests. People want to protect their own money and bank their own exposure. The role of government is to maintain the integrity of and confidence in the whole system. With electronic cash, just as with paper cash today, it will be the responsibility of government to protect against system risk. This is serious role that cannot be left to the micro-economic interests of commercial organizations”. The security of information may be one of the biggest concerns to the Internet users. For electronic banking users who most likely connect to the Internet via dial-up modem, is faced with a smaller risk of someone breaking into their computers. Only organizations such as banks with dedicated internet connections face the risk of someone from the internet gaining unauthorized access to their computer or network. However, the e-banking system users still face the security risks with unauthorized access into their banking accounts. Moreover, the e-banking system users also are concerned about non-repudiability which requires a reliable identification of both the sender and the receiver of on-line transactions. Non-secure electronic transaction can be altered to change the apparent sender. Therefore, it is extremely important to build in non-repudiability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates.

There are a multitude of possible scenarios where sensitive data can be stolen or misplaced when processing an online transaction. The methods used to steal and compromise sensitive data is dynamic and ever changing. Their purpose is to target applications and architectures that are widely used, such as instant messaging, email, standardized shopping carts, redundant coding schemes, database programs, and security techniques and encryption. Security concerns should be discussed during the design stages of systems development to ensure it is addressed properly (Chorafas, 2004). One reason for the multitude of security concerns faced by users is that the internet was not developed with security in mind, thus many of the techniques security professionals are putting into place are reactionary and hackers are using these same methods. Traditional E-commerce security can be broken down into a three-tier model where the client, server, and database are described separately (Shwan, 2006). To gather an understanding for the threats against E-Commerce applications, we must also explore security concerns that threaten all systems.

Attacks on E-Banking

The Kenyan Prime Bank, Development bank, and CFC Stanbic Bank websites which were hacked by Rwandan hacker is one example of how the system is vulnerable to hackers. Hackers have many different ways that they can try to break into the system. The problems of the systems today are inherent within the setup of the communications and also within the computers itself. The current focus of security is on session-layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels, and a trustee code at both endpoints. It is really important to have a secure protocol because the trusted channels really don’t exist in most of the environment.

There are various types of attacks that e-banking can suffer. They include

1. Social Engineering

One of the most common attacks does not involve knowledge of any type of computer system. Tricking consumer s into revealing sensitive information by posing as a system administrator or customer service representative is known as social engineering. Social engineers use surveillance and a consumer’s limited knowledge of computer systems to their advantage by collecting information that would allow them to access private accounts.

2. Port Scanners

Attackers can use port scanners to ascertain entry points into a system and use various techniques to steal information. This type of software sends signals to a machine or router and records the message the machine responds with to ascertain information and entry points (Cobb, 2007). The main purpose of a port scanner is to gather information related to hardware and software that a system is running so that a plan of attack can be developed.

3. Packet Sniffers

The connection between a user's computer and the web server can be "sniffed" to gather an abundance of data concerning a user including credit card information and passwords. A packet sniffer is used to gather data that is passed through a network (Bradley, 2005). It is very difficult to detect packet sniffers because their function is to capture network traffic as they do not manipulate the data stream. The use of a Secure Socket Layer connection is the best way to ensure that attackers utilizing packet sniffers cannot steal sensitive data.

4. Password Cracking

Password cracking can involve different types of vulnerabilities and decrypting techniques; however, the most popular form of password cracking is a brute force attempt. Brute force password attacks are used to crack an individual's username and password for a specific website by scanning thousands of common terms, words, activities, and names until a combination of them is granted access to a server. Brute force cracking takes advantage of systems that do not require strong passwords, thus users will often use common names and activities making it simple for a password cracker to gain access to a system. Other password cracking methods include using hash tables to decrypt password files that may divulge an entire systems user name and password list.

5. Trojans

Trojan software is considered to be the most harmful in terms of E-Commerce security due to its ability to secretly connect and send confidential information. These programs are developed for the specific purpose of communicating without the chance of detection. Trojans can be used to filter data from many different clients, servers, and database systems. Trojans can be installed to monitor emails, instant messages, database communications, and a multitude of other services. The percentage of personal computers with Trojan software installed was a staggering 31% in 2006 with a steady increase from years before (Webroot, 2006).

6. Denial of Service Attacks

Denial of service attacks are used to overload a server and render it useless. The server is asked repeatedly to perform tasks that require it to use a large amount of resources until it can no longer function properly. The attacker will install virus or Trojan software onto an abundance of user PC's and instruct them to perform the attack on a specific server. Denial of service attacks can be used by competitors to interrupt the service of another E-Commerce retailer or by attackers who want to bring down a web server for the purpose of disabling some type of security feature. Once the server is down, they may have access to other functions of a server, such as the database or a user's system. This allows the attacker the means to install software or disable other security features.

7. Server Bugs

Server bugs are often found and patched in a timely fashion that does not allow an attacker to utilize the threat against an E-Commerce web site. However, system administrators are often slow to implement the newest updates, thus allowing an attacker sufficient time to generate a threat. With the millions of web servers in use around the world, thousands often go without timely patches, leaving them vulnerable to an onslaught of server bugs and threats (Khusial, McKegney, 2005).

8. Super User Exploits

Super user exploits allow attackers to gain control of a system as if they were an administrator. They often use scripts to manipulate a database or a buffer overflow attack that cripples a system, much like a Denial of Service attack for the purpose of gaining control of the system. Users can create scripts that manipulate a browser into funneling information from sources, such as databases.

Despite the various attacks on e-commerce, there are various defenses as (Khusial, McKegney, 2005) noted below.

a) Education

Your system is only as secure as the people who use it. If a consumer chooses a weak password, or does not keep their password confidential, then an attacker can pose as that user. This is significant if the compromised password belongs to an administrator of the system. In this case, there is likely physical security involved because the administrator client may not be exposed outside the firewall. Users need to use good judgment when giving out information, and be educated about possible phishing schemes and other social engineering attacks.

b) Personal firewalls

When connecting your computer to a network, it becomes vulnerable to attack. A personal firewall helps protect your computer by limiting the types of traffic initiated by and directed to your computer. The intruder can also scan the hard drive to detect any stored passwords.

c) Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is a protocol that encrypts data between the consumer’s computer and the site's server. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents.

The SSL certificate is issued to the server by a certificate authority authorized by the government. When a request is made from the consumer’s browser to the site's server using https://..., the consumer’s browser checks if this site has a certificate it can recognize.

d) Server firewalls

A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines.

A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. This allows the client browser to communicate with the server. A second firewall sits behind the e-Commerce servers. This firewall is heavily fortified, and only requests from trusted servers on specific ports are allowed through. Both firewalls use intrusion detection software to detect any unauthorized access attempts.

Another common technique used in conjunction with a DMZ is a honey pot server. A honey pot is a resource (for example, a fake payment server) placed in the DMZ to fool the hacker into thinking he has penetrated the inner wall. These servers are closely monitored, and any access by an attacker is detected.

e) Password policies

Ensure that password policies are enforced for consumer s and internal users.

f) Intrusion detection and audits of security logs

One of the cornerstones of an effective security strategy is to prevent attacks and to detect potential attackers. This helps understand the nature of the system's traffic, or as a starting point for litigation against the attackers.

Suppose that you have implemented a password policy: If a consumer makes 6 failed logon attempts, then his account is locked out. In this scenario, the company sends an email to the customer, informing them that his account is locked. This event should also be logged in the system, either by sending an email to the administrator, writing the event to a security log, or both.

You should also log any attempted unauthorized access to the system. If a user logs on, and attempts to access resources that he is not entitled to see, or performs actions that he is not entitled to perform, then this indicates the account has been co-opted and should be locked out. Analysis of the security logs can detect patterns of suspicious behavior, allowing the administrator to take action.

In addition to security logs, use business auditing to monitor activities such as payment processing. You can monitor and review these logs to detect patterns of inappropriate interaction at the business process level.

The infrastructure for business auditing and security logging is complex, and most likely will come as part of any middleware platform selected to host your site

Conclusion

The internet has grown exponentially, with more than 2,267 million which is actually 32.7% of the world population in December 2011. The internet enhances the interaction between two businesses as well as between individuals and business. As a result of the growth of the internet, electronic commerce has immerged and offers tremendous market potential for today's business. One industry that has benefited from this new communication channel is the banking industry. Electronic banking (e-banking) is offering its customers with a wide range of services. Customers are now able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions. E-banking is offered by many banking institutions due to pressure from competitions. Today, it is believed that people make the difference to information technology and security development and that training on the ethical, legal and security aspects of information technology usage should be ongoing at all levels within organizations (Nolan, 2005).

The future of electronic banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard. Most research studies have indicated that the common problem affecting information security and privacy of customers is e-services provider's lack of security control which allows damaging privacy losses. Apart from that, another problem is the subsequent misuse of consumers' confidential information, as in identity theft. These may affect customer's confidence toward online business transaction in a variety of privacy risk assessments by consumers. Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the consumer to be vigilant when doing business online.

References:

1. F. Westin (1967), Privacy and Freedom, Athenaeum, New York.
2. Albrechtsen, E. (2007) A qualitative study of user's view on information security. Computer and Security 26 (4): 276–289.
3. M. K. Cheung, & M. K. O. Lee (2006), “Understanding Consumer Trust in Internet Shopping: A Multidisciplinary Approach” Journal of the American Society for Information Science and Technology, vol. 57, no. 4, pp. 479-492
4. Debar H. and Viinikka, J. (2006) Security information management as an outsourced service. Computer Security 14 (5): 416–434.
5. Dhillon, G. (2001) Challenges in managing information security in the new millennium. In: G. Dhillon (ed.) Information Security Management: Global Challenges in the New Millennium. Hershey, PA: Idea Group Publishing, pp. 1–8.
6. Dhillon, G. and Torkzadeh, G. (2006) Values-focused assessment of information system security in organizations. Information Systems Journal 16 (3): 293–314.
7. F. Belanger, J.S. Hiller & W.J. Smith (2002), (“Trustworthiness in Electronic Commerce: the Role of Privacy, Security, and Site Attributes” Journal of Strategic Information Systems, vol. 11, pp. 245–270
8. Leach, J. (2003) Improving user security behavior. Computers and Security 22 (8): 685–692.
9. N. K. Malhotra, S. S. Kim, J. Agarwal (2004), “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model” Information Systems Research, vol. 15, no. 4, pp. 336-355
10. Nolan, J. (2005), Best practices for establishing an effective workplace policy for acceptable computer usage. Information Systems Control Journal 6 (2): 32–35.
11. Parker, Donn B., (2004) Toward a new framework for information security, in Computer Security Handbook, 4th edition, Bosworth, Seymour and Kabay, M. E. (eds.), John Wiley and Sons.
12. Pfleeger, Charles P. (1997) Security in Computing. Prentice Hall.
13. S. Davies, “Big Brother (1996): Britain’s web of surveillance and the new technological order”, London. p. 23.
14. S. Warren, & L. Brandeis (1890), “The Right to Privacy” Harvard Law Review 4.
15. T. Singh, & M. E. Hill (2003), “Consumer privacy and the Internet in Europe: a view from Germany” Journal of Consumer Marketing, vol. 20, no. 7. pp. 634-651
16. V. Shankar, G. L. Urban, & F. Sultan (2002), “Online Trust: a Stakeholder Perspective, Concepts, Implications, and Future Directions” Journal of Strategic Information Systems, vol. 11. pp. 325-344
17. Bradley, Tony. *Introduction to Packet Sniffing*. 2005. <http://netsecurity.about.com/cs/hackertools/a/aa121403.htm> (accessed 5/3/2012)
18. http://www.centralbank.go.ke/downloads/bsd/annualreports/bsd2010.pdf (accessed 5/3/2012)

19. http://www.cofek.co.ke/index.php?option=com_content&view=article&id=959:mobile-ohone-now-drives-consumer-spending&catid=1:latest-news (accessed 8/3/2012)
20. http://www.fincen.gov/news_room/rp/files/e-cash.pdf (accessed 5/3/2012)
21. http://www.information.go.ke/index2.php?option=com_docman&task=doc_view&gid=23&Itemid=37(accessed 5/3/2012)
22. http://www.internetworldstats.com/emarketing.htm (accessed 7/3/2012)
23. http://www.krio.me/internet-security-threats-and-protection-methods/ (accessed 12/2/2012)
24. http://www.networkworld.com/news/2008/100108-government-sends-auditors-to-investigate.html?fsrc=rss-security (accessed 15/3/2012)
25. http://www.palgrave-journals.com/rm/journal/v13/n1/full/rm20113a.html (accessed 12/3/2012)
26. http://www.standardmedia.co.ke/InsidePage.php?id=2000041790&cid=457&currentPage=1 (report published 29/8/11, Kenya Scores high in electronic banking).(accessed 29/8/2011)
27. http://www.webroot.com/resources/stateofspyware/excerpt.html
28. Khusial, McKegney, 2005: e-Commerce security: Attacks and preventive strategies http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html (accessed 20/3/2012)