ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

THE IMPACT OF INFORMATION SECURITY MANAGEMENT FOR E- BANKS PERFORMANCE IN KINGDOM OF SUDI ARABIA

Bushra Mohamed Elamin Elnaim (Assistant professor)
Department Of Computer Science and Information, College of Science and Humanity Studies-Alsulial,
Prince Sattam Bin Abdulaziz University, Kingdom Of Saudi Arabia.

DOI: 10.5281/zenodo.166827

ABSTRACT

Information security is a great concern to computer users, which is not only a technical problem, but also related to human factors. One of the main issues in Kingdom of Saudi Arabia related to Internet banking is the weak security in Internet banking application. Therefore this study will investigate further the solution to enhance the security issues in Internet banking implementation. In today's high speed world, millions of transactions occur every minute. For these transactions, data need to be readily available for the genuine people who want to have access, and it must be kept securely from imposters. Information security is measured by the degree of the application of ISO 27001 and PCI-DSS standards on Saudian Banks, while banks' performance is measured by indicators of profitability and asset quality. This paper aims to comprehensively identify and assess the information security management for e-banks in Saudi Arabia with an attempt to fill the gap in the literature.

KEYWORDS: **E-**banking, Information Security Management, Security Requirements, Saudian Banks.

INTRODUCTION

Banking industry is considered one of many businesses that have taken advantages of the Internet and IT development by introducing Internet banking service to their customers that brings many benefits to banks and customers (Kasemsan and Hunngam, 2011, Aladwani, 2001)(1,2). Internet banking processes have given banks customers the full power to control their bank accounts from any place with the availability of the Internet at anytime (Gurau, 2002)(3). The secret of the Internet banking that attracts many customers is "the round-the-clock availability and ease of transactions and avoidance of queues and restrictive branch operating hours" (Al-Somali. et al, 2009)(4). The number of users using online banking continues to growth along with the number of Internet users around the world. In terms of Saudi Arabia, it is considered the largest Arab country in the number of customers using Internet banking services, where it is more than 12 million customers perform online banking operations worth around SR470 billion on the Internet annually (NAFFEE, 2011) (5).

Recently banks started offering online banking services to their consumers, but some of them did not feel safe to deal with their confidential information online. However the main reasons for the customer’s concerns are lack of security and usability awareness. Security and usability are the most important factors that can affect the adoption of the online banking services anywhere .All banks in Saudi Arabia are using online banking; providing their customers with the ability to access their bank accounts and make transactions anytime and anywhere. In contrast, online banking has revealed some types of security threats that can endanger the use of such services; since customers provide very confidential information and exposing such information would affect the customer as well as the bank relationship with their customers (6). The employees of three major Saudi Banks; NCB (Alahli), Alrajhi Bank, Riyad Bank, are the concern of this survey**.**

LITERATURE REVIEW

Below are brief definitions of the main concepts of the research

1- Information Security

Information security means protecting information and information system from unauthorized access, use, disclosure, disruption, modification or destruction (Feruza & Kim, 2007) (7). It can increase information security in the banking sector by providing certain goals available such as the availability, integrity and confidentiality.

2- **Information security management** (ISM) describes controls that an organization needs to implement to ensure that it is sensibly managing these risks. (8)

The risks to these assets can be calculated by analysis of the following issues:

- *Threats to your assets*: These are unwanted events that could cause the deliberate or accidental loss, damage or misuse of the assets
- *Vulnerabilities*: How susceptible your assets are to attack
- *Impact*: The magnitude of the potential loss or the seriousness of the event.

3- E-banking

E-banking, also known as **internet banking**, **Online banking** or **virtual banking**, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services. Fundamentally and in mechanism, online banking, internet banking and e-banking are the same thing. (9)

Internet banking types:

According to SAMA (Saudi Arabian Monetary Agency), (2010) (10), there are three types of Internet banking which are:

1-Informational-only websites: which only offer information about the bank‘s services and products.

2-Information transfer websites: these types are used as communicative platforms between the bank and its customers in order to transmit some documents or applications such as loan applications.

3-Fully transactional websites: these types provide the abilities for all previous types. They have the high level functionality that allows customers to execute financial transactions which is done usually a connection between customers' devices and banks' internal systems.

The need for information security in businesses

Information is the primary commodity in world of E-Commerce. As technology advances and access to markets expand, the need to protect information to ensure its confidentiality, integrity, and availability to those whom need it for making critical personal, business, or government decisions becomes more important. (11)

Security Requirements

These requirements are categorized into administrative security requirements, and technical security requirements [Manual of secure networks, information systems and international business institutions, 2002] (12).

Administrative Security Requirements

According to the manual of secure networks, information systems and international business institutions, 2002, there are 9 principles of Administrative Security Requirements, categorized as follows:

a) Basic principles:

- awareness
- liability
- response

b) Social principles:

- ethics
- democracy.

c) Principles of security phases:

- risk assessment
- security design and implementation
- security management
- revaluation

Technical Security Requirements

Include security requirements for electronic systems and [Abdelgadir, 2007] (13):
a) Security of Resources
b) Physical security
c) Technical security
d) Network security and software security

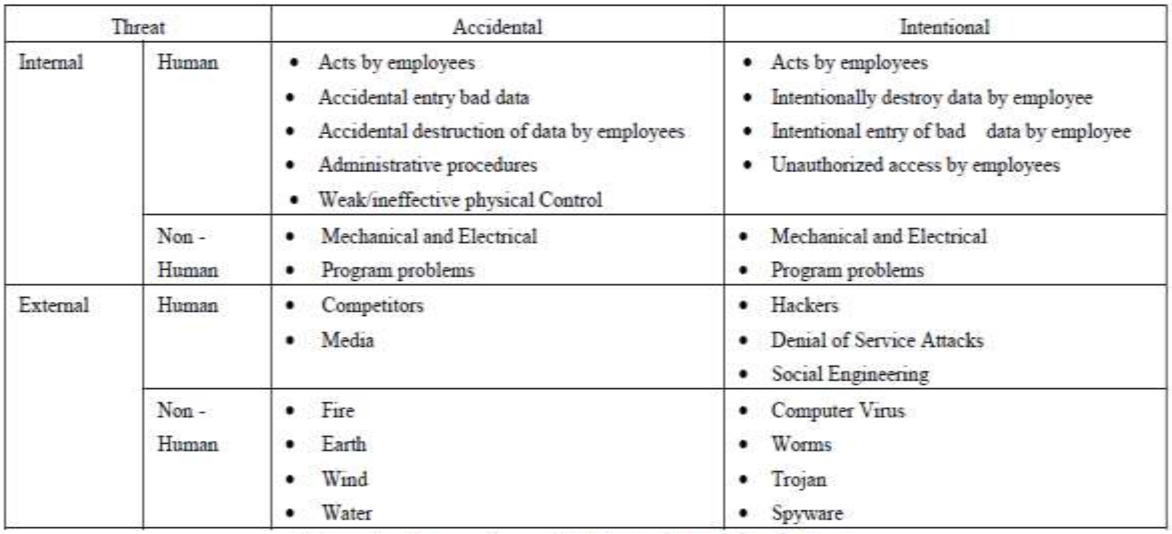
There is a need for a set of standards to ensure the best security practices are adopted and an adequate level of security is attained .There are several standards which lead to information security such as ISO 27001, PCI-DSS and COBIT. Susanto et al. (2011) (14) classifies information security management system standards as follows:

- ISO 27001: ISO is the international standard that describes best practice for an information security management system (ISMS). Accredited certification to ISO 27001 demonstrates that an organization is following international information security best practices. (15)
- PCI-DSS: Short for ***P****ayment* ***C****ard* ***I****ndustry* (PCI) ***D****ata* ***S****ecurity* ***S****tandard*(DSS), PCI DSS is a standard that all organizations, including online retailers, must follow when storing, processing and transmitting their customer's credit card data.(16) The ***D****ata* ***S****ecurity* ***S****tandard* (DSS) was developed and the standard is maintained by the ***P****ayment* ***C****ard* ***I****ndustry* ***S****ecurity* ***S****tandards* ***C****ouncil* (PCI SSC). To be PCI complaint companies must use a firewall between wireless network and their cardholder data environment, use the latest security and authentication such as WPA/WPA2 and also change default settings for wired privacy keys, and use a network intrusion detection system.
- COBIT: **COBIT** (**Control Objectives for Information and Related Technologies**) is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance. COBIT provides an implementable "set of controls over information technology and organizes them around a logical framework of IT-related processes and enablers." (17)

Information Security Risks for E- Banking

In terms of information security risks, the identification of risks and their impact is a complicated process due to the complexity of technology, the sophistication of security attacks and the lack of historical information regarding some certain risks. So, it is the responsibility of banks management to do risks management regularly and taking appropriate security controls (SAMA, 2010; MAS, 2008). (18,19)

The source of the risk can be natural, human error, technical, environmental (Bessis, 2002) (20). Natural source such as electric shock and floods; human error such as misconfiguration; technical such as viruses or deficiencies in the information system ; environmental risks relate to all aspect that relate to banking environment such as regulations, employees, and policies. Figure (1) shows many threats that affect to information security in banks as follows:



Threat		Accidental	Intentional
Internal	Human	• Acts by employees • Accidental entry bad data • Accidental destruction of data by employees • Administrative procedures • Weak/ineffective physical Control	• Acts by employees • Intentionally destroy data by employee • Intentional entry of bad data by employee • Unauthorized access by employees
	Non - Human	• Mechanical and Electrical • Program problems	• Mechanical and Electrical • Program problems
External	Human	• Competitors • Media	• Hackers • Denial of Service Attacks • Social Engineering
	Non - Human	• Fire • Earth • Wind • Water	• Computer Virus • Worms • Trojan • Spyware

Figure 1. Types of security threats in banking industry

Source:(French,2012) (21)

RESULTS AND DISCUSSION

Several questions were asked to Saudi banks staff. The questions focused on the awareness of e-bank's policies and penalties and measures to detect violations. Saudian banks usually inform their employees of information security policies. However, the results show that 81% of the participants are aware that their e-banks have a security policy and less than 40% of the participants have been trained on how to maintain the information security. In fact, 94% of participants are aware that they have IT security teams in their banks. This leads to the conclusion that IT managers of organizations utilize the information security teams effectively.

The analysis shows that 87% of participants are sure who to contact in case they detect a virus or any malicious software or a hacking attack. As far as awareness of attacks and threats are concerned, only 40% of the participants are generally careful while opening an email attachment, only 38% are aware of fishing attacks and 30% are aware of email spams and their identification. This leads to the conclusion that employees are not well trained to be aware of common threats in the IT sector which include email spams and attachments as well as fishing attacks.

As far as violations are concerned a variety of questions were asked which included transfer of confidential information, downloading or installing software on company machines, use of official information at home using e-banks accounts and logging in to e-banks accounts from public computers like cyber cafes and hotel lobbies. 28% of the participants can use their mobile phones and other personal devices to store or transfer confidential e-bank information. 25% of the participants have downloaded and installed software on official machines without realizing the severity of risks involved. However, 10% of the participants take official information and use computers at home to work on it regularly and 35% agreed to do the same but occasionally. These results support the fact that 50% of the employees agreed that they partially follow policy rules of their organization and 10% participants either don't follow the policy rules at all or are not aware if any such policy exists.

In addition, limited usage policies regarding websites and personal emails are not well known to the majority of the participants. 50% of the participants are not aware if any email usage policy exists in their organization and 80% are aware if there are any policies limiting visits to certain websites. This leads to the conclusion that e-bank policies are well circulated among the employees.

Also this Analysis was made as to why and under what circumstances violation of information security policy was made. 14% of the participants agreed that they violated the company policies as there was no other choice to complete a task and 13% of the participants violated to complete the task within the tight deadline schedules. There were 29% of the participants who agreed that violating information security policy compensates good job performance. Even though the percentages are less, the organizations must take such violations seriously and encourage alternative methods. Because 51% of the participants perceive that violation of security policies help them save work time and 30% of the participants feel that it saves effort.

CONCLUSION

E- banking is one of the most useful services provided by banks to their customers. It brings many benefits to banks, such as reducing costs, increasing competition and increasing profits. In terms of customers, it is possible for them to carry out financial transactions from anywhere and at any time**.** The following conclusions are based on the findings of this study:

- The bank needs to have IT-related strategy and policies.
- There needs to be an annual review of IT strategy and policies taking into account the changes to the organization's business plans and IT environment**.**
- Bank-wide risk management policy or operational risk management policy needs to be incorporate IT-related risks also. The Risk Management Committee periodically reviews and updates the same (at least annually).
- Banks must concern the internal risks, such as interest in external risks.
- Accessing the Internet by the staff should be controlled.
- Training the bank's customers on the safe use of their accounts

REFERENCES

1. Kasemsan, M. and Hunngam, N.(2011). Internet Banking Security Guideline Model for Banking in Thailand. *Communications of the IBIMA*.
2. Aladwani, A.M.. (2001). Online banking: a field study of drivers, development challenges, and expectations. *International Journal of Information Management* **21** (3), 213–225.
3. Gurau, C. (2002). Online banking in transition economies: the implementation and development of online banking systems in Romania. *International Journal of Banking.***20** (6), 285-296.
4. Al-Somalim, S., et. al. (2009). An investigation into the acceptance of online banking in Saudi Arabia. *Technovation.* **29**, 130-141.
5. Naffee, I. (2011). *Saudi banks take out campaign to educate customers about hackers.* [Online], Arab News. Available from : http://arabnews.com/saudiarabia/article472462.ece [Accessed 28 June 2016].
6. Monzer M. Qasem, " Developing a Robust Evaluation Framework to Evaluate Security for Online Banking Services ", International Journal of Advance Research in Computer Science and Management Studies(IJARCSMS), Paper ID: V2I10-0065, Volume 2, Issue 10, October 2014, ISSN (Online) : 2321-7782, ISSN (Print): 2347 – 1778, Scientific Journal Impact Factor is 4.739 (SJIF-2013), International Society for Research Activity Impact Factor is 1.473 ((ISRA -2013) India.
7. Feruza, S., & Kim, T. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering,2*(2).
8. Available on https://en.wikipedia.org/wiki/Information_security_management accessed at 06/07/2016.
9. Available on https://en.wikipedia.org/wiki/Online_banking accessed at 06/09/2016.
10. SAMA. (2010). *E-banking Rules* [Online]. Saudi Arabia: SAMA. Available from http://www.sama.gov.sa/sites/samaen/RulesRegulation/Rules/Pages/E_banking_Rules.docx [Accessed 20/6/2016].
11. Available on https://www.sans.org/reading-room/whitepapers/awareness/information-security-todays-economy-916 accessed at 06/10/2016.
12. *"Information Security for Executive Managers. Towards Culture of Security'.* A Manual of Securing Networks & Information Systems for International Business Institutions in Accordance & The Foundation of The Organization for Economic Cooperation and Development (OECD), 2002 .
13. Abdelgadir, Howaida Ali. "Management Information Systems: Theory and Practice", Sudan University of Science and Technology, 1st ed., 2007
14. Susanto, H., Almunawar, M.,& Taun, Y.(2011). Information Security Management System Standards: A Comparative Study of the Big Five.*International Journal of Electrical & Computer Sciences,11*(5).
15. Available on http://www.itgovernance.co.uk/iso27001.aspx?404;http://www.itgovernance.co.uk:80/iso27001.asp
16. Available on http://www.webopedia.com/TERM/P/PCI_DSS.html accessed at 8/10/2016.

17. Available on https://en.wikipedia.org/wiki/COBIT accessed at 10/10/2016
18. SAMA. (2010). *E-banking Rules* [Online]. Saudi Arabia: SAMA. Available from http://www.sama.gov.sa/sites/samaen/RulesRegulation/Rules/Pages/E_banking_Rules.docx [Accessed 20 July 2016].
19. Mas. (2008). *Internet Banking and risk management*. [Online]. Monetary Authority of Singapore. Available from http://www.mas.gov.sg/resource/legislation_guidelines/risk_mgt/IBTRMV3.pdf [Accessed 10 July 2016].
20. Bessis, J. (2002). *Risk Management in Banking.* Second Edition, England: John Wiley & Sons Ltd.
21. French, A. (2012). A Case Study on E-Banking Security-When Security Becomes Too Sophisticated for the User to Access Their Information. *Journal of Internet Banking and Commerce*,*17*(2).