International Journal of Economics and Finance; Vol. 7, No. 9; 2015
ISSN 1916-971X E-ISSN 1916-9728
Published by Canadian Center of Science and Education

The Impact of Information Security on Banks' Performance in Egypt

Nader Alber[1] & Myvel Nabil[1]

[1] Ain Shams University, Cairo, Egypt

Correspondence: Nader Abler, Associate Professor, Faculty of Commerce, Ain Shams University, Cairo, Egypt. Tel: 201-005-668-507. E-mail: naderalberfanous@yahoo.com

Received: May 20, 2015 Accepted: June 16, 2015 Online Published: August 25, 2015

doi:10.5539/ijef.v7n9p219 URL: http://dx.doi.org/10.5539/ijef.v7n9p219

Abstract

This paper attempts at investigating the impact of information security on the performance of Egyptian banks. This has been conducted using a sample of 13 banks (out of 32 banks), during 2013. Information security is measured by the degree of the application of ISO 27001 and PCI-DSS standards on Egyptian Banks, while banks' performance is measured by indicators of profitability and asset quality.

ISO 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS). Besides Payment Card Industry Data Security Standards (PCI-DSS) is a comprehensive standard is intended to help organizations protectively protect customer account data.

Results indicate that implementation of ISO 27001 standards may affect profitability indicators as measured by "Return on Capital", while implementation of PCI-DSS standard may affect asset quality as measured by "Non-Performing Loan Ratio".

Keywords: asset quality, Egyptian banks, information security, information security Management System (ISMS), ISO27001 certification, PCI-DSS standard

1. Introduction

The internet banking services operate their businesses depending on the development of banking services and modern technology. On the other side, the threats and security breaches highly increase in recent years. Some banks have already faced some security threats represented in Trojan virus, Spam, Spyware/malware, Hacking and stealing information etc. Therefore, the banking industry as a whole should be aware enough to accommodate the issue of information security in its own strategic policies.

Hilal (2015, p. 186) addresses that new information and communication technologies (NICT) has already led to: (1) technology supported logistically the internal processing of information and networks by developing interbank networks and (2) Second, NICT-based new systems fastened the access to capital markets.

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

To serve the purpose of any information system, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. Integrity means that data cannot be modified undetectably. Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.

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) classifies information security management system standards as follows:

- ISO 27001: ISO, founded on February 23, 1947, the international standard of ISO 27001 specified the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organization. The standard introduced a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model.

- PCI-DSS: The Payment Card Industry Data Security Standard (PCI-DSS) is a worldwide information security standard defined by the Payment Card Industry Security Standard Council. The standard was created to help industry organizations processes card payments and to prevent credit card fraud through increased controls around data and its exposure to compromise.
- COBIT: The Control Objectives for Information and related Technology (COBIT) is a certification created by the IT Governance Institute (ITGI) in 1996. They believe that it is a set of practices (framework) for IT management.

Besides, there is a need for these standards to avoid information security threats and the resulting losses. Glaessner et al. (2003) addresses that some incidents in banking sector due to information security threats, as follows: In 1995, Citibank witnessed loss of $10 million due to an intrusion into the financial entity's networks. Besides in 2001, Gorshov and Ivanov had access to Central Texas Bank's system for six months before they were detected. After that in 2002, Unidentified Bank and Citibank incurred steal $141000 from online accounts. In 2003, Italian Banking System witnessed stole the credit card information of an estimated 5000 customers. In addition, a Malaysian crime ring hacked into the Nebraska Bank's computer system, attacking the visa check card program.

Recently, Price Water house Coopers "PWC" survey 2014 revealed that banks targeted by cyber criminals with 39% of financial sector falling victim to cybercrime compared with 17% in other industries (Price Water house Coopers, 2014b). 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).

Each standard has its own role and position in implementing Information Security Management System. Several standards such as ISO 27001 focus on information security management system, while PCI-DSS focus on information security relating to business transactions and smart card, in addition to COBIT focus on information security and it relation with the project management and IT Governance (Susanto et al., 2011).

Many researchers great concern with online banking security, the security issues internet banking are facing today, framework for the governance of information security in banking system, information security threats in banks, and compare security systems of different type of banks in several countries, But in Egypt research on information security in banks is still in its infancy. To our knowledge, there's no study regarding the impact of information security on the performance of Egyptian banks.

Regarding economic crime, Price Water house Coopers (2014a) indicated that the Middle East region presented a unique situation, as it reported the lowest of all, where those respondents who did report fraud indicated a high number of types and instances of fraud.

Table 1. Economic crime reported by region

Territory	Reported Fraud 2014	Reported Fraud 2011
Africa	50%	59%
North America	41%	42%
Eastern Europe	39%	30%
Latin America	35%	37%
Western Europe	35%	30%
Asia Pacific	32%	31%
Middle East	21%	28%
Global	37%	34%

Source: Price Water house Coopers (2014a).

In brief, this study tries to answer these two main questions:

- Does information security affect banking performance, as measured by profitability indicators?
- Does information security affect banking performance, as measured by asset quality?

The paper is arranged as follows: after this introduction, section 2 reviews research literatures that has concerned with "information security" and" information security in financial institutions", while section 3 explains how to measure research variables and investigates how to test the research hypotheses. Section 4 illustrates the empirical work, presents results, and discusses how these results answer research questions using multiple regression analysis and Chi-square test and section 5 summarizes the paper and provides remarks about conclusions.

2. Literature Review

This section tries to present some of previous work that has been conducted in two fields: 1) information security and 2) information security in financial institutions.

Regarding information security, Susanto et al. (2011) introduces various information security standards and provides a comparative framework for major information security standards, namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT. This study sheds some lights on the position and specialization of each standard, and on the adoption and usability levels in different countries.

Kumar and Puri (2012) examines the elements that need to be considered when developing and maintaining information security policy of various universities. The authors show strategies that can be used in order to: (1) deal with information threats along with risk management and present a design for a suit of information security policy and (2) cover authentication, cryptography, access control, back up and system security management.

Concerning with information security in financial institutions, Khan and Barua (2009) illustrates the state of information security and its challenges. The study uses both primary data (a questionnaire with 40 questions) and secondary data (different online and physical sources). Results show that banking sector in Bangladesh is sufficiently vulnerable of different information security threats, as it tends to use many IT based platforms in regular business.

Altamimi (2011) indicates that Saudi banks focus on external risk more than internal risk, bank' employees are more confident from being protected from external attacks than internal attacks. Ambhire and Teltumde (2011) introduces the concept of information technologies in financial and banking industries, analyze the relationship of information technology risk factors, and provide investigation information system security in the context of internet banking. Results assure the importance of security in financial transactions.

Ula et al. (2011) shows the information assets and potential threats for banking system. A comprehensive information security governance framework is highly needed for banking information system. Some general standards and best practices have been developed such as FFIEC, COBIT, ISO 27002 and PCI data security standard as the framework is categorized into strategic, tactical, operational, and technical levels.

Siddique and Rehman (2011) represents a conceptual framework of the basic crimes occurred in banks- namely ATM frauds, money laundering and credit card fraud. Results conclude that to elimination of cybercrime is not a possible task, while it is possible to have a regular check on banking activities and transactions. Therefore, the study suggests some changes in the Information Technology Act, to reduce cybercrimes.

Jassal and Sehgal (2013) attempts to explore several of technology and security standards required for safe

internet banking and to analyze the performance of ICICI Bank, OBC Bank and HSBC Bank, based on the recommendations given by RBI for secure online banking. Result show that cyber criminals try different techniques for getting unauthorized access to finances of financial institutions, banking customers.

Comparing with previous work, most studies have focused on assessment and causes of information security risk, while the current study concerns with its standards and effects. Besides, most of papers - in this field - are technical-oriented, while the current one is financial-oriented.

3. Data Description and Hypotheses Developing

Data about ISO 27001 & PCI-DSS standards have been collected using a questionnaire to find out the level of application, as shown in table (2). ISO 27001 standard includes the following items (Salah & Hinson, 2009):

- Identify the policies and objectives of information security management system through information gathering, analysis and the development of a specific strategy and security program to achieve the goals.
- The degree of application of this system to all areas at risk.
- Plan to address risks, develop standards and prepare risk reports.
- Monitoring is follow-up processes and setting key performance indicator (KPI) to measure it.
- Monitoring and control through global standards that can be measured and applied.
- Define Responsibilities and procedures of internal accounting and administrative responsibility through specific matrix of responsibilities, activities and duties of each individual.
- Plan of process of risk mitigation (Change Management).
- Methods and procedures for the protection and prevention from information security threats.

For each of the preceding items application level should be addressed as not designed**,** designed, allocated, drafted, or approved.

The procedures of PCI-DSS standard could be represented as follow (PCI Security Standards Council LLC, 2010):

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly updated anti-virus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need to know.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

For each of the preceding items application should be addressed as applied or not applied**.** Required data regarding information security, Profitability and asset quality indicators could be shown as follows:

Table 2. Variables representing information security

Variable	Sign	Calculation
ISO 27001 standard	ISO	= the average of ISO items.*
Requirements of Payment Card Industry Data Security Standard (PCI-DSS)	PCI	= the average of PCI items. **

* Source: Salah & Hinson (2009). For each item, ISO = 1, if it's not designed, = 2, if it's designed, = 3, if it's allocated, = 4, if it's drafted and = 5, if it's approved.

** Source: PCI Security Standards Council LLC (2010). For each item, PCI = 0, if it's not applied and = 1, if it's applied.

Required data regarding profitability and asset quality could be shown as follows:

Table 3. Variables representing profitability and asset quality

Variable	Sign	Calculation
Return on Assets	ROA	Net Profit / Assets
Return on Equity	ROE	Net Profit / Equity
Return on Capital	ROC	Net Profit / Capital
Non-Performing Loans Ratio	NPL	Loans Loss Provisions / Total Loans
Stock' Market Return	SMR	$(Price_t - Price_{t-1}) / Price_{t-1}$

This Paper aims at testing the following two hypotheses:

- There is no significant effect of information security on bank performance as measured by profitability indicators.
- There is no significant effect of information security on bank performance as measured by asset quality.

Regarding the effect of information security on profitability indicators, the null hypothesis H0, for each of ISO and PCI, could be shown as:

$$\beta_{ISO} = 0 \quad (1)$$

$$\beta_{PCI} = 0 \quad (2)$$

The alternative hypothesis Ha could be shown as:

$$\beta_{ISO} \neq 0 \quad (3)$$

$$\beta_{PCI} \neq 0 \quad (4)$$

4. Results of Empirical Study

The following table illustrates descriptive statistics of information security, profitability and asset quality indicators for a sample of 13 banks (out of 32 banks in Egypt), during 2013.

Table 4. Descriptive statistics of information security, profitability and asset quality

Variable	N	Minimum	Maximum	Mean	Std. Deviation
ISO	89	1.0000	5.0000	3.07632	1.6999115
PCI	103	0.0000	1.0000	0.64466	.3867228
ROA	87	-0.0818	0.0285	0.00766	.0184251
ROE	87	-1.4040	.4022	.057149	.3127977
ROC	87	-.4926	.9267	.212684	.2609193
NPL	82	.0000	.8000	.168293	.2083907
SMR	61	-.7529	1.1514	.043934	.4689803

Source: Outputs of data processed by researchers.

To test the significance of information security effect on banking performance, we used step-wise regression technique. The following table illustrates the results, as follows:

Table 5. Effects of information security on profitability and asset quality

Dependent variable	R^2	F	β_{ISO}	β_{PCI}
ROA	---	---	---	---
ROE	---	---	---	---
ROC	**0.550**	**14.674**	**0.063**	---
	(0.257)	(0.002)***	(3.831)***	
NPL	---	---	---	---
SMR	---	---	---	---

Note. Values under R^2 standard error and values under F represent level of significance. Values under B coefficients, between brackets, are t values, while *, **, and *** represent levels of significance 10%, 5%, and 1% consequently.

The above-shown table indicates that null hypothesis could be rejected for the first hypothesis. So, the alternative hypothesis may be accepted. This means that ISO27001 standard (ISO) may affect rate of return on capital (ROC). To test the second hypothesis, Chi-square test has been conducted and provided the following results, as follows:

Table 6. Effects of information security on profitability and asset quality

Dependent variable	Chi^2_{ISO}	Chi^2_{PCI}
ROA	1.942	7.753
	(0.508)	(0.866)
ROE	1.942	7.753
	(0.508)	(0.866)
ROC	1.942	7.753
	(0.508)	(0.866)
NPL	1.857	1.407
	(0.933)	(0.000)***
SMR	---	---

Note. Values under Chi-square represent level of significance, where *** represents levels of significance at 1%.

The above-shown table indicates that null hypothesis could be rejected for the second hypotheses. So, the alternative hypothesis may be accepted. This means that Requirements of Payment Card Industry Data Security Standard PCI-DSS (PCI) may affect asset quality as measured by Non-Performing Loan (NPL) using Chi-square test.

Results indicate that ISO 27001 standard (ISO) may affect rate of return on capital (ROC) as shown in Table 5, and requirements of payment card industry data security standard PCI-DSS (PCI) may affect Non Performing Loan (NPL) as shown in Table 6.

5. Summary and Concluded Remarks

This paper attempts to investigate the impact of information security on the performance of Egyptian banks. This has been conducted using a sample of 13 banks, during 2013. Information security is measured by the extent of the application of ISO 27001 and PCI-DSS standards in Egyptian Banks, while banks' Performance measured by profitability and asset quality indicators.

Results indicate that implementation of ISO 27001 standards may affect profitability as measured by Return on Capital, while implementation of PCI-DSS standard may affect asset quality as measured Non-Performing Loan Ratio. Market seems to have no response to information security, as bank stock price has not been affected by ISO neither by PCI. This has to be more elaborated through further researches to investigate how informational content about information security may affect stock price.

References

Akhavein, J., Frame, W., & White, L. (2005). The diffusion of financial innovations: An Examination of The Adoption of Small Business Credit Scoring by Large Banking Organizations. *Journal of Business 78*, 577-596. http://dx.doi.org/10.1086/427639

Altamimi, T. (2011). *Information Security Risks for Internet Banking in Saudi Arabia*. A study submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Systems at the university of Sheffield.

Ambhire, V., & Teltumde, P. (2011). Information Security in Banking and Financial Industry. *International Journal of Computational Engineering & Management, 14*. Retrieved from http://www.ijcem.org101

Bonnette, C. (2003). *Assessing Threats to Information Security in Financial Institutions*. GSEC Certification Practical Assignment, Version 1.4b - Option 1 Retrieved from http://sans.org

Emmanuel, A. (2011). *The Effect of Internet Banking on the Ghanaian Banking Industry: A Case of CAL Bank, UNI Bank and PRUDENTIAL Bank*. A Thesis Submitted to the Institute of Distance Learning, Kwame Nkrumah University of Science and Technology in partial fulfillment of the requirement for the degree of commonwealth executive master of business administration.

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).

Frei, F., Harker, P., & Hunter, L. (1997). *Innovation in Retail Banking*. Working Papers # 97-48, Financial Institutions Center, The Wharton School, University of Pennsylvania.

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).

Glaessner, T., Kellermann, T., & Mcnevin, V. (2002). *Electronic Security: Risk Mitigation in Financial Transactions Public Policy Issues*. World Bank Policy Research Working Paper 2870, p. 8. http://dx.doi.org/10.1596/1813-9450-2870

Glaessner, T., Kellermann, T., & Mcnevin, V. (2004). *Electronic Safety and Soundness Securing Finance in a New Age*. World Bank Policy Research Working Paper, No. 26, pp. 79-86.

Hilal, M. (2015). Technological Transition of Banks for Development: New Information and Communication Technology and Its Impact on the Banking Sector in Lebanon. *International Journal of Economics and Finance, 7*(5), 186-200. http://dx.doi.org/10.5539/ijef.v7n5p186

Jassal, R., & Sehgal, R. (2013). Comparative Study of Online Banking Security System of Various Banks in India. *International Journal of Engineering, Business and Enterprise Applications*. Retrieved from http://www.iasir.net

Khan, M., & Barua, S. (2009). The Status and Threats of Information Security in the Banking Sector of Bangladesh: Polices Required. *Bangladesh Journal of MIS, 1*(2).

Koskosas, I., Kakoulidis, K., & Siomos, C. (2011). A Model Performance to Information Security Management. *International Journal of Business and Social Science, 2*(4).

Kumar, S., & Puri, A. (2012). A Framework for Evaluation and Validation of Information Security Policy. *International Journal of Computers and Distributed Systems, 1*(3). Retrieved from http://www.ijcdsonline.com

PCI Security Standards Council LLC. (2010). *PCI DSS Attestation of Compliance for Onsite Assessments*. Merchants Version 2.0. Retrieved from https://www.pcisecuritystandards.org/.../pci_dss_aoc_merchants.doc

Price Water house Coopers. (2014a). *Economic Crime: A threat to business globally*. Retrieved from http//www.pwc.com/crimesurvey

Price Water house Coopers. (2014b). *Threats to the financial Services Sector.* Retrieved from http//www.pwc.com/crimesurvey

Siddique, I., & Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector-An Overview. *International Journal of Business & Information Technology, 1*(2).

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).

Ula, M., Ismail, Z., & Sidek, Z. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cyber Security*. http://dx.doi.org/10.5171/2011.726196

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).