Journal of Practical
Management Information Systems

J. Practical MIS, 1(4): 11-20, 2020

Research Paper

Influence of Security Information Management in Cyber Environment on Electronic Banking Efficiency

Mehrnaz Paknezhad

[a] Cinnagen Pharmaceutical Company, Tehran, Iran
Faculty of Humanities, Payam -e- Noor University, Zanjan, Iran

Received: 20 June 2020 Accepted: 26 July 2020 Published: 17 August 2020

Abstract

The nature of crimes and abuse committed in new cyber environment causes anxiety with regard to protection of financial information . Insufficient security of technology together with its virtual nature, gives a good opportunity to profiteers. Thus, the effect of financial information security in cyber environment on the functionality of e-banking systems is considered for analysis. Therefore, statistical population in this research, are managers and experts of informatics section of banks of Zanjan city and sample population was equal to This research with regard to objective is practical and with regard to research design is descriptive survey, regarding the level of variable measurement, Pearson correlation test was used for the analysis of relationship between variables and regression analysis was used for analysis of type and form of relation.

The results of analysis show that there is a meaningful relationship between information security of cyber environment and e-banking functionality.

Keywords: Information security – financial-cyber – e-banking.

How to cite the article:
M. Paknezhad, Influence of Security Information Management in Cyber Environment on Electronic Banking Efficiency, J. Practical MIS, 2020; 1(4): 11-20,

Introduction

Financial Information systems have an important role in achieving objectives of every organization, one way to achieve these objectives would be through providing security in information systems; today, security in financial information systems has become so much important that managers always try to apply the most recent information technology for development and security of their information systems. Financial information systems can increase and organization value. One way that financial information systems can add to the commercial institute value is to provide correct and timely information to perform different activities. A financial information system which is correctly designed and is secure can increase efficiency and effectiveness of these activities through correct related and timely information to beneficiaries. One of the primary objectives of financial information system is to help the management for controlling commercial institute. Achieving security and sufficient control of information resources of an organization should be one of the primaries of senior manager of each organization. When manager is not sure enough of the security of correct flow of information, certainly he cannot perform his duties effectively by relying on that information and achieve the organization and his own objectives (Vadyei, 2010). Duty of information systems is to process information but sometimes it is assumed that, what happens in information systems of organizations is just a simple processing of raw primary information of financial and non-financial which are effective on organization activities but the reality is that managers at different levels encounter with different issues that because of the complexity of problem-solving methods are at different degrees and kinds of systems that can help this variable collection at a range of common past-oriented information systems rather than intelligent future-oriented systems in which discussion of security establishment is considerable (Arab Mazar, 2006). Controlling information systems is a necessity, especially in cases that this system is not sufficiently secure (Aria, 2001). In companies and firms that information security system is weak, danger of penetrating to this system and manipulating information is high, damages can be irrecoverable. Need for information security requires managers make necessary predictions so that the information system be properly secured and the information be reliable. Thus, security in information systems of banks with regard to change in new approaches of banks toward presenting new services and e-banking is an important discussion. In line with this, bank managers need to assure their customers and always try to increase security in financial systems (Vadiei, 2010). Nowadays, in bank environments and financial and monetary institutes, users can access any information services of e-banking without considering the fact that this information is located in what part of the world. Cyber environment provides ground for important economic activities and a necessary tool for doing all commercial transactions at international level provides for human being at every time and place. The zone of users is not limited to physical borders of a house and even borders of a country and at a low cost level, any user can meet people around the world and deal information, without knowing the real place identity of people. The nature of crimes and abuse committed in new cyber environment leads to anxiety for keeping financial information. Insufficient technology security together with its virtual nature provides a good opportunity for profit seekers. The most worrying aspect of cyber space is to protect financial information in virtual space for banks. Therefore the main question is that how the financial information security in cyber environment influence the functionality of e-banking systems.

Definition of security and the term "information security"

In a dictionary the word "security" means surviving danger, security, and relief from fear or concern. The word "information security" means keeping security and information systems against illegal access and use of it (Safaie, 2004). Thus, lack of information security causes concern and anxiety for organizations and commercial or non-commercial units, including banks and financial in. Therefore, providing security for information systems is in order for the following objectives: 1. Comprehensive information: reliable information is information that is complete, comprehensive and flawless. Thus, information could not be manipulated by illegal people. For this end, information should be kept against danger of any change including; increase, decrease or illegal pollution intentionally or accidentally. 2. Confidential information: illegal natural or legal persons should not be able to access information and use it illegally. 3. Legal use of information: information should be applied in legal ways by legal people. Therefore, any user is only permitted to use information to a legal extent and for specific purposes. 4. Accessibility of information: information should be available to legal users on time and quickly. Legal user should be able to access information at a time he needs it (Aria, 2001). Thus, managers of banks and financial and monetary institutes should make sure that their organization provides information security through the following ways: a) Evaluation of possibility of danger and level of loss that can be derived from illegal assessing, using, disorder, reformation or destruction of such information or information systems. b) Determination of the level of relative information security to prevent damage of such information or information system according to standards. c) Applying policies and process to decrease affordable costs and the possibility of danger to an acceptable level. d) Examining and evaluating techniques and controls of information security to make sure that they are performed effectively (Vadiei, 2010). Efficiency of financial information systems in the area of banks and financial institutes depends on the quality of services provided, i.e. any weakness or lack of security in financial information systems leads to reduction in efficiency, effectiveness and irrecoverable damages and losing customers etc.

Literature Review

According to Deloitte‟s 8th global financial services industry security survey, 57% of respondents of more than 250 financial services organizations from 39 countries that were surveyed increased their information security budgets last year. In Asia Pacific, including Australia but excluding Japan, that figure stood even higher at 73%.Over the course of the last few years, there has been a number of large scale losses resulting from information breaches. This has driven home the importance of strong security processes. At the same time, the digitization of the economy has increased vulnerability to attacks, driving the search for better protection. Although, one in three financial institutions in Asia Pacific including Australia endured a privacy related breach in the last year, in the U.S half of all financial institutions were breached, and in the UK more than two out of three financial services organizations were breached. We have seen some global situations where financial institutions have suffered hundreds of millions of dollars‟ worth of losses due to fraud. As we digitize more, we connect more devices to our systems, and as customers become more online-reliant, the environment is becoming increasingly conducive to financial crime. Tommy Viljoen (2012-. Rok

Bojanc presents a comprehensive model for managing information-security risks that allows an evaluation of the investments in security and the protection of business-information systems. The model is based on a quantitative analysis of security risks and allows an evaluation of different investment options in information security. The model is designed as a standard procedure that leads an organization from the initial input data selection to the final recommendations for the selection of an optimum measure that reduces a certain security risk (Rok Bojanc, 2013).The study attempted to examine the use of information systems data security tools and on-line usage of databases amongst the banking and insurance companies operating in the region. Difference in the use of the identified items was observed based on their size, nature of the data processing activity and the level of the reporting hierarchy. In general, it has been found that the use of information systems tools and techniques varies along each of the above mentioned dimension. It has been found that sometimes smaller firms earning less revenue were also making use of some techniques which the larger organizations were not making use of. That is to say that the use of these techniques is independent of the size of the company. The companies having more centralized structures have been more frequent users of the data security techniques and on-line databases as compared to the ones which were either decentralized or mix of both. The degree and extent of usage of on-line usage also varies with the reporting hierarchy. The companies reporting to the lower levels had higher security controls and make more frequent use of on -line databases. In today‟s competitive scenario information systems offer more advantages that are unparalleled and the firms can exploit this to their advantage by leveraging IT. The firms must continually evaluate their systems strengths and ascertain their impact (Versha Mehta, 2006**)**. Min Jae Lee‟s research examined the negative impact of an Internet hacking incident in which an online shopping site‟s customer records were stolen by an external hacker. The study first tested whether or not an information security incident can actually trigger any negative responsive behaviors against the compromised online vendor, and then established the concept and measure of reiterative behaviors. This study also developed a theoretical model that can explain reiterative behaviors, and empirically test the developed model using survey data collected from online shoppers who had experienced an information security incident. (MinJae Lee, 2010**)**. The European Union (EU) focuses on the protection of the data of natural and legal persons in order to keep e-services safe and sound.

EU legal acts which determine the financial payment involving data and information security standards and criteria are important for all EU Member States. Ebanking systems ensure a prompt and adequate performance of safe financial transactions. Statistical data are analyzed in order to evaluate the situation, i.e. to find out how virtual currency transfers and payments for goods and services using e-instruments are increasing on a large scale. Technological development of epayment increases the possibilities of quick and qualitative transfers, but cyber-security requirements and their implementation technologies are essential issues to be considered. Despite all security measures, threats to the security of e-payments are real and very serious. Systems „cracking‟ tools and techniques are no less technologically advanced than their countermeasures. Most developed countries around the world pay much attention to the security of „sensitive‟ information. One of the categories of this kind of information is financial data Dalė Dzemydienė discusses risk factors in assessing safety measures for financial payment. The authors analyze some ways in which software and hardware measures can be used for retrieving personal data by falsifying e-payment instruments, misleading the users of financial systems and directing them to websites with dangerous content (Dalė Dzemydienė, 2010). In order to develop e-commerce services, internet banking needs to codify a security process. This issue needs designing an effective method for protecting users within internet environment. A suggested framework in relation with the way of identifying internet banking security needs should be able to secure transactions in dangerous environments. E-commerce basically concentrates on information. E-commerce includes a wide range of activities that includes two sets of institute to customer and institute to institute. Industries such as banking warmly welcome e-commerce for gaining competitive advantages. There are four integrated factors to globally accelerate internet banking: 1- more demands to accelerate, 2- Intense competition between banks and newcomers 3- banks‟ attempt to reduce costs and reaching to new levels of efficiency 4- Deregulation of service market. Statistics show that ATMs, telephonebanks and in-home banking include more than 50 percent of all bank transactions and all ex-branch activities increase up to 15 percent every year (Hatchinson, 2000). Heiko Gewald showed that BFI manager‟s attitude changes according to the perception of risk magnitude. The ranking of the individual risks per risk facet provides valuable insights into the causes and drivers of risks. In particular, the formation of strategic risk with its individual risks adds to the scarce knowledge of the possible outcomes of outsourcing on a bank‟s flexibility and innovativeness. Thus, BFI managers may use our formatively measured strategic risks to assess the impact of outsourcing on their institutional agility. The theoretically deduced and empirically tested indicators are not only useful for scholars calibrating future surveys, but also for risk managers trying to identify the causes and drivers of overall outsourcing risks. Managers in the BFI may use these results to construct risk assessment tools – such as cause-effect-models– which guide risk analysis within the outsourcing decision process. The findings of this study also offer insights to readers in charge of service provider operations into the „gut feelings‟ of their clients.(Heiko Gewald-2006).Today, cyber is the fifth field after earth, sea, air and space. Given the cyberspace entering all aspects of life from scientific issues to work, entertainment, economy, education and communications, attackers can create challenges in the target society‟s people‟s daily affairs. Moreover, as most organizational or inter-organizational communications are made through internet, cutting the internet service itself could be a reason for challenges and inconvenience in countries. Hence, setting a harmonic and united strategy in cyberspace in local, national and international levels is a must. (Seyed Vahid Aghili, 2013).

Methodology

This research is applied regarding objective and with regard to research design is descriptive survey. The objective of applied research is to develop applied nowledge in a particular field. In other words, applied research leads to scientific application of knowledge. And descriptive research includes a collection of methods whose aim is to describe conditions with phenomena under study. Implementing descriptive research can only be for the purpose of more familiarity with present conditions or voting to decision making process. Most of researches in behavioral science can be considered as descriptive research.

Research hypotheses

This research has one main hypothesis and four sub-hypotheses as follows:

Main hypothesis

Financial information hypothesis in cyber environment affects functionality of e-banking systems.

Sub-hypotheses

1. There is a significant relation between primary actions for managing information security and success of managing financial information security.
2. There is a significant relation between organization decisions for managing information security and success of managing financial information security.
3. There is a significant relation between accessing to necessary sources for managing information security and success of managing financial information security.
4. There is a significant relation between operation management for managing information security and success of managing financial information security.

Statistical population

Statistical population of this research are manager and experts of Informatics section of Zanjan city banks out of which several people should be studied with regard to problems and hurdles and through smaller adding and with a certain method to find out the features of a society and finally the obtained results are generalized to the entire society. Since the statistical population in this research is managers and experts of informatics section of Zanjan banks who are divided into two groups of informatics managers and experts, from each class, people are randomly selected, in fact sampling method is categorized. In this research we calculate sample population by Cochran formula.

$$n=\frac{\dfrac{z^2pq}{d^2}}{1+\dfrac{1}{N}\left(\dfrac{z^2pq}{d^2}-1\right)}$$

In this formula:
n= sample population
N= statistical population that equals to 321.
Possibility of first type error (a) equals to 5%, as a result Z (a/2) =1.96, P=0.5 and q=0.5 (relative community) that is equally determined. The accepted error (d) calculated equals to 5%. According to this formula, sample population equals to 175. 200 questionnaires were distributed from which 176 questionnaires returned to the researcher flawless and correctly and analysis operation was performed on them. The tools for assessing this research were questionnaire whose questions were posed in two expert group (related to research variables) and demographic group with 33 questions. Questions of expert group evaluate the relationship between each indicator of managing financial information security in cyber environment and success of its function in e-

banking. Questions are adopted from questionnaire of Hal *et al*. research article (2011) with some changes.

Table 1: Questions about research hypotheses

Research variables	Questions
Primary actions	1 to 6
Organization decisions	7 to 13
Access to required resources	14 to 20
Operation management	21 to 24
Success in function	25 to 29
Demographic variables (position, job history, education, information access)	30 to 33

Questions of this questionnaire were in closed form and in a 5 degree Likert scale and in form of totally agree (5), agree (4), neither agree nor disagree (3), agree (2), totally disagree (1). The questionnaire validity was also assessed. By validity we mean, questions in this questionnaire examine exactly variables and subject under study, i.e. as much as possible data collected through questionnaire are not more than the researcher‟s needs and at the same time part of data needed related to assessing variables in examination are not deleted and reality is as it is shown, the amount of circumstantial evidence KMO shows the meaningful level of Kerroit Bartlett. For KMO, amounts lower than 0.5 shows trivial factor analysis, 0.5 to 0.7 shows average factor analysis, 0.7 to 0.8 shows balanced factor analysis, 0.8 and higher shows desirable factor analysis. For the present data amount of KMO obtained, shows a suitable factor analysis.

Table 2: Circumstantial evidence KMO

Variable Primary actions	Organization	decisions	Access to necessary	resources	Operation
KMO	0.73	0.66	0.60	0.77	0.73

Reliability of questionnaire was also tested. Reliability refers to accuracy, trustworthiness, stability or being repeatable of test results. To measure questionnaire‟s reliability, at first a number of 30 consumers were randomly chosen and after distributing, gathering and analyzing data, questionnaire reliability was calculated using Cronbach alpha for each variable and the entire questionnaire.

Table 3: Reliability coefficient of questionnaire

Variable	Primary	actions	Organization	decisions	Access to necessary	resources
Cronbach alpha	0.61	0.72	0.73	0.76	0.79	0.87

According to the table above all dimensions have Cronnbach alpha higher than 0.6 and the total average equals to 0.87 that shows desired reliability of questionnaire.

Data analysis

In this research, in order to analyze data SPSS software version 21 was used. Analysis of research questions was performed at two levels of inferential and descriptive statistics. At the descriptive part, statistical analysis including frequency, percentage is used along with tables and figures. In inferential statistics with regard to the level of variable measurement Pearson correlation test was used for analyzing the relationship between variables and regression analysis was used for analyzing type and form of relationship. Descriptive findings of this research includes frequency table and percentage of individual characteristics of sample people and statistical descriptive indicators like average, standard deviation and variance that if needed for all variables under study is presented in this research.

Table 4: Frequency distribution according to job history

Job history	frequency	Real percentage
Under 10 years	77	43.8
11 to 20 years	87	49.4
Over 30 years	12	6.8
Total	176	100

Findings of table 4 show that 77 people less than 10 years (43.8 percent), 87 people (99.4 percent) up to 20 years and 12 people (6.8) have over 30 years of job history. Findings of table 5 show that 10.2 percent (18 people) of sample population have diploma, 15.9 percent (28 people) have associate degree, 60.2 percent (106 people) have bachelor degree and finally 13.6 percent (24 people) have master‟s degree and higher.

Table 5: Frequency distribution based on respondents' educational degree

Education	frequency	Real percentage
Under diploma	0	0
diploma	18	10.2
Associate degree	28	15.9
Bachelor degree	106	60.2
Total	176	100

Table 6: Results of Pearson correlation test

Variables	**Management success**	**Correlation** coefficient	**Meaningful level**
	Primary actions	0.39	0.00

As table 6 shows, significance level of correlation test is lower than 0.05, thus, there are sufficient reasons for rejecting null hypothesis, i.e. there is a significant relationship between independent variable of primary actions and success in managing information security; also regarding the fact that the correlation coefficient is positive, the variables are aligned.

Hypothesis testing

Testing first hypothesis

First hypothesis states that there is meaningful relationship between primary actions for information security management and success in managing financial information security.

H0: $\rho=0$
H1: $\rho \neq 0$

Second hypothesis testing

The second hypothesis indicates that there is a significant relationship between decisions of organization to manage information security and success in managing financial information.

H0: $\rho = 0$
H1: $\rho \neq 0$

Table 7: Results of Pearson correlation test

Variables	Management success	Correlation oefficient	Significance level
	Organization decisions	0.77	0.00

As table 7 shows, Significance level of correlation test is lower than 0.05, thus there are enough reasons to reject null hypothesis, i.e. there is a significant relationship between independent variable of organization decisions and success in managing information security; also with regard to the fact that the correlation coefficient is positive, the variables are aligned.

Testing the third hypothesis

The third hypothesis states that there is significant relationship between access to necessary resources for managing information security and success of managing financial information security.
H0: ρ =0
H1:ρ≠0

Table 8: Results of Pearson correlation test

Variables	Management success	Correlation coefficient	Significance level
	Access to necessary information	0.60	0.00

As table 8 shows, significance level of correlation test is lower than 0.05, thus there are enough reasons to reject null hypothesis, i.e. there is a significant relationship between independent variable of access to necessary information and success in managing information security; also with regard to the fact that the correlation coefficient is positive, the variables are aligned.

Testing forth hypothesis

The fourth hypothesis states that there is a significant relationship between operation management for information security and success in managing financial information security.
H0: ρ =0
H1:ρ≠0

Table 9: Results of Pearson correlation test

Variables	Management success	Correlation coefficient	Significance level
	Operation management	0.22	0.005

As table 9 shows, significance level of correlation test is lower than 0.05, thus there are enough reasons to reject null hypothesis, i.e. there is a significant relationship between independent variable of operation management and success in managing information security; also with regard to the fact that the correlation coefficient is positive, the variables are aligned. With regard to the results obtained, we find out that the intensity of correlation between managing financial information security and organization decision making has the highest amount and operation management has the lowest amount. One of the most important discussions in data analysis and statistics is awareness of the relation between variables under study. Regression analysis of the type of relationship between variables, examines the prediction and adherence of a variable from other variables.

Table 10: Primary information about regression

Model	Variables entered into model	Inactive variables	Method
1	0	M, action, resource, ta	

a: All requested variables entered.

The above table provides overall information about regression model used for data. Independent variables entered into model are variables of primary actions, decision making, necessary esources and operation management. The chosen method for entering variables is "Enter" and the dependent variable of success model is management of financial information security that is specified in the table. The above table represents indicators of evaluatingmodel including multiple correlations®, de termination coefficient (R square) and balanced determination coefficient and standard deviation of these indicators. Determination coefficient is a percentage of dependent variable changes that is indicated by dependent variable, for the present data, since the amount of indicator equals to 0.63, thus, the model is able to explain 63 percent of changes in success of managing financial information security in e-banking. The remaining percentage is related to other factors that are studied in this research. Regarding the undesirable effect of entrance of some variables with an insignificant effect, the amount of determination coefficient reduces from 0.62 to 0.61.

Table 11: Multiple correlation coefficient and determination coefficient

Model	multiple correlation coefficient	determination coefficient	Balanced determination coefficient	Standard deviation method
1	0.791	0.626	0.616	0.83901

Table 12: Variance analysis

Model	Total square	df	Mean square	F	Sig.
Regression	898.783	4	224.969	66.440	0.0
Remaining	537.729	159	3.382		
Total	1436.512	163			

The above table shows the regression variance analysis. This model includes dependent and independent variables. Since probability of test significance is less than 0.05, regression model is significant i.e. this model is able to predict dependent variable;in other words at least one of independent variables is effective in predicting dependent variable. So, each independent variable should be tested by T-test.

Table 13: Regression coefficient

Model	Non-standard coefficients		standard coefficients	t	Sig. Lower Bound	95.0% Confidence Interval for B	
	B	Std. Error	Beta			Upper B Bound	
Y-intercept	-1.815	1.098		-1.652	.100	-3.984	.355
Action	-.118	.061	-.120	-1.930	.055	-.239	.003
Decision	.551	.053	.675	10.382	.000	.447	.656
making							
Resources	.191	.048	.259	3.955	.000	.096	.287
Operation	-.001	.017	-.004	-.083	.934	-.035	.033
management							

In column B, the amount of y-intercept and regression non-standard coefficient was presented; the amount of positive effect of each independent variable on the dependent variable. Beta non-standard coefficient indicates the amount of change in dependent variable per each unit change in independent variable. With regard to the significance probability of test for regression coefficient, y-intersect and primary action variables and operation management are not significant (sig> 0.05). i.e. they cannot predict success in managing financial information security (a=0 , b=0). Regression coefficient is significant for significance coefficient and necessary resources (sig> 0.05). i.e. per each unit increase in necessary resources, 0.26 units increase occurs in success of financial information security and per each unit change in organization decisions about information security, 0.67 units change happens in the success of financial information security.

$Y= 0.67\, t + 0.26\, m$

t: decision making
m: necessary resources
Y: managing financial information security

Conclusion and suggestions

Information security for an important part of activists in information technology section is presented as an acute issue only when a problem occurs in system. Most of the times, this problem cause a heavy blow on the system or to the available information. Infact, it can be said that it is a delayed approach. Internet has always been criticized and evaluated from different angles but the truth is this huge system like any other typical human society encounters dangers and threats. From penetration of destructive data to destruction of healthy data and disturbing the order of system all together is dependent on just one thing and it is discussing about the information security in through internet environment. Any selling or buying on the internet or transferring data should be done under a security control. If the security of network is not established, its numerous advantages would not be achieved and money and e-commerce, services to particular users, personal information, public information and e-journals all will be manipulated and abused both materially and immaterially. Also, manipulation of information – as a foundation for nations thinking – by international organized groups, is considered a kind of disturbing national security and invasion against governments and a national threat. In Iran that most of basic software like operating system and applied and internet software, are provided by intermediaries and foreign companies, there is a fear of penetration through hidden ways. Now, banks and most of organs and other institutes act through net, so preventing the penetration of destructive factors in net is shaped as a strategic issue that ignoring it will lead to damages. There are also experiences in this field that totally proves this subject. With regard to the results obtained in this research it can be said security of financial information in virtual space greatly affects efficiency of e-banking systems and internet banking. But, because global net web represents new achievements everyday, also suitable approaches should quickly be provided to maintain security. Thus, future researches to analyze these approaches and new issues in the area of information technology can greatly help maintaining financial information.

There are some ways which can be suggested to maintain security in this research by banks and expected by customers as follows:

- Clarity of web address verified by monetary and financial institute in bank journals.
- Verification of website through digital licenses.
- Preserving PIN and password.
- Using mouse or touch screen buttons with stimulus sensitive information.
- protection against the virus.
- Implementing a firewall.
- an at least 128-bit encryption.

Setting limitation for customers who are not identified within web and limitation for access to codes.

The following cases are represented for increasing trust of e-commerce users‟ and electronic banks to do economic and commercial activities: *Preservation* : a process through which it is assured that customers are satisfied to give their information to data collectors.

Verification: it means to assure customers that transactions made through websites are done with real and main site of the bank he desires.

Confirmation: by confirmation we mean a third group is present as observer to testify transactions are done between which people, in other words activity in internet is guaranteed this way.

Dismiss denial: a mechanism to make sure that PC (Client) is connected to the bank server and vice versa. Thus, the participants in this regard won‟t be able to deny their activity. Banks and financial; and monetary institutes and commercial institutes by implementing a security strategy which benefit the following advantages:

- Increasing bank and e-banking customers by increasing customers‟ confidence in financial institutes.
- Profitability of more monetary institutes which increase by attracting customers‟ capital.
- Reduction of the probability of systems and programs inactivation.
- Effective use of human and non-human resources in a monetary institute (increase in profit).
- Reduction of the cost of losing data by destructive viruses and or security cavities (preserving valuable data).
- Increasing preservation of intellectual property.
- Owning a strategy for managing risks in necessary times.

A security problem that causes loss of customers‟ information can lead to legal implications for a monetary institute.

References

[1] Arab Mazar Yazdi, M. (2006). Application of Expert Systems in Accounting Education; Proceedings of the Eighth National Accounting. Publisher Marandiz, pp. 53 -66.

[2] Arya, N. (2001). Auditing Computer Networks, Publication No. 152, Accounting organizations, First Edition.

[3] Bojanc, R., & Jerman-Blažič, B. (2013). A Quantitative Model for Information-Security Risk Management, *Engineering Management Journal,* 25 (2), 25-37.

[4] MinJae Lee & JinKyu Lee (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet, *Inf Syst Front*, 14, 375– 393.

[5] Safaei, A. (2004). Network Security, publisher of Danesh Parvar.

[6] Vadyie, M.H., & Mohammadi, J. (2010). Financial Security in Information Systems. *Auditor Journal,* 51.