Modern Security Applications for Banks and Accounting Information Systems

Mohammed Kasiem Shariza (Lecturer)*

Abstract

The Widespread use of the Internet has completely re-defined the nature of information security. All companies now generally and banks particularly face global threats to their networks, and, more importantly, to their accounting data and information. The number of Internet security incidents reported increased every year.

The previous facts lead us to this research. The objective of this research is to evaluate the Modern Security Applications for Banks and Accounting Information Systems. An empirical survey-using questionnaire was conducted to achieve the above-mentioned objective

The research results shows that banks use Modern Security Applications also shows that banks has lack in Accounting Information Systems.

The main recommendation for this research is to increase training strength in all directions in accounting information systems to minimize possible threats that may appear.

Keywords: Modern Security Applications, Information Security, Accounting Information Systems.

*Al- Mansour University College

1-Introduction and Research Methodology

The information security and protecting it in banks generally and Accounting Information Systems (AIS) particularly is common goal of maximizing the effectiveness of the banks efforts to protect its information resources, the task of developing and managing proper modern security applications involves a host of complex behavioral issues which will be highlighted in this research.

AIS is a system or group of systems that collects and processes data and information, which measured in terms of money. AIS process accounting transactions and provide information for the interested users that used to make decisions and help management to perform business activities properly. AIS are the oldest and the widest used information systems in business. AIS based on the double entry bookkeeping concept. Accounting is primarily concerned with the design of the system of records, the preparation of reports based on the recorded data and information, and the interpretation of the reports to the both internal and external users to help both making decision. Accounting system is a recording process system like journal, ledger, worksheet, trial balance and procedures that are produced reliable and relevant information.

The world is full of threats, which generally classified as hardware, software, data, information and communication lines as well as network threats. The banks must put in place adequate measures to ensure the protection of information assets through effective policies, controls, and standardized procedures and control testing. This would ensure the reduction in threats to banks and AIS.

1- The research objective:

The objective of this research is to evaluate the modern security applications for banks and AIS as an attempt to confront and minimize existing threats.

2- The research problem:

The banks and AIS faces many threats as a common result of technology development, that effects negatively on banks businesses generally and AIS particularly.

3- The research hypotheses:

The research identify the following hypotheses, which provide solution to the problem raised before: (The uses of modern security applications in banks and AIS reflects positively on banks businesses generally and AIS particularly)

4- The research importance:

The importance of this research raises in the following points:

1-Highlight how important modern security applications for banks and AIS

2-Evaluate the security applications used in banks and AIS

3-Review the most common security threats exist on banks and AIS

2- Previous Researches

1- Research of (Bawaheh, Shamsi S., 2014) research title (Information security for Organizations and Accounting Information Systems: A Jordan Banking Sector Case)

The objective of this research was studying the dramatic changes that are occurring in the accounting environment such as the new technologies, which have an impact on many financial statement filings, new services that accountants are involved in and the need for specialized online database research skills that are continuously expanding.

As one of the important conclusion of this research was, it is important to remember that it is not enough just to establish a series of controls; someone or some department must be accountable for the control and the security of the network. This includes being responsible for developing controls, monitoring their operation, and determining when they need to be update or replaced.

This research recommend to banks implementing controls, or defense mechanisms which should designed to protect all of the components of an information system, including data, software, hardware, and networks.

2- Research of (Neogy, Taposh Kumar, 2014) research title (Evaluation of Efficiency of Accounting Information Systems: A Study on Mobile Telecommunication Companies in Bangladesh)

The research aim was to set up the foundation of the statistical analysis. Researcher has selected two mobile telecommunication companies out of six mobile telecommunication companies in Bangladesh for the research study.

A research most important result was that existence of internal control system increases the efficiency of AIS through ensuring safeguarding of assets, reliability of accounting information, accuracy of accounting information.

The research also recommended that it is important to separate operation and accounting because separation in mobile telecommunication companies increases the efficiency of AIS because it ensures correct processing of transactions without manipulation of figure.

3- Research of (Goreva at.el., 2013) research title (Exploring Accounting Information Systems and Embezzlement from Nonprofit Originations)

The aim of this research is to identify and describe how nonprofits use accounting software and manage risk in their organizations.

The result of this research was motivation is primarily for financial reasons, often resulting from low salaries or even no salary in the case of volunteers (very typical for nonprofits). The way employees rationalize their behavior may affect their compliance with security policies.

The research recommended the nonprofits begins to focus on the magnitude of potential losses from fraud and embezzlement, this would be a first step in improving their risk management activities. By recognizing that the development of embedded accounting software controls would complement risk management activities and ethics policies, software vendors would be encouraged to adopt these features.

4- Research of (Muhrtala and Ogundeji, 2013) research title (Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case)

The objective of the research was to provide evidence on the existence of threats in the Computerized Accounting Information Systems (CAIS) of companies in Nigeria.

A research most important result was that factors such as accidental entry of bad data by employees, accidental destruction of data by employees, employees sharing of log-on credentials, introduction of virus, unauthorized access to information systems and unauthorized documents visibility via display on monitors and hardcopy documents are the most significant security threats to computerized accounting information systems.

The research also recommended that organizations should endeavor to implement substantial security measures to protect IT infrastructure using physical, logical, environmental and administrative (policies, guidelines, standards, and procedures) controls.

3- Accounting Information Systems (AIS) in Banks and Information Security

Spiceland at.el. (2016: 52) Stated that accounting information systems businesses actually use are quite different from company to company and from bank to bank. Larger companies or banks generally use more complex systems than smaller companies or banks use. The types of economic events affecting companies also cause differences in systems. This point of view supported also by Kieso at.el. (2013: 84) which he defined AIS as following;

(Collects and processes transaction data and then disseminates the financial information to interested parties. Accounting information systems vary widely from one business to another. Various factors shape these systems: the nature of the business and the transactions in which it engages, the size of the firm, the volume of data to be handled, and the informational demands that management and others require)

In the same time Hall, (2011:7) look to AIS as subsystems process financial transactions and nonfinancial transitions that directly affect the processing of financial transactions.

All the above points shows that AIS is systems, main systems, different systems or even subsystems it all met and agree on the word system that helps any

organization in collecting different data , process it and distribute them to decisions makers. AIS needs technology to be accurate, reliable and in time line too. The right arm to execute the AIS missions in any organization is Information Security. Understand the term information security and the benefits to banks and AIS of being proactive in dealing with security risks such as: adopting an information security policy with respect to handling sensitive data, having procedures for reporting security incidents, making staff members aware of their responsibilities.

Information security refers to all the procedures, which are used to protect information for deliberate or accidental misuse or dissemination. Technically, it refers to the maintenance of the integrity of information. Integrity means that the information remains correct at all times and cannot be accessed by unauthorized agents (Varley, 2006:55).

There is a whole dark area to business known as industrial espionage in which a variety of means are used to discover trade secrets and business dealings. Obviously, there is an absolute imperative to maintaining the confidentiality of all company information. A less obvious breach of information security occurs through industrial espionage where

Information is either changed or deleted to sabotage the functioning of the organization (Varley, 2006:55-56).

4- Threats Facing Banks and Accounting Information Systems (AIS)

When the issue of information security is at stake, three fundamental concepts must be taken into consideration (Garzia, 2013:449):

1. Confidentiality
2. Availability
3. Integrity.

These objectives will help to clarify what should generally be protected and the reason for doing this.

The attacks against confidentiality of information are related to the theft of or unauthorized access to data. This can happen in many ways, such as the interception of data while it is in transit or simply the theft of devices on which the data are stored. The objective of compromising confidentiality consists of obtaining proprietary information, the use of credentials, disposing of secret, financial, health-related or other type of information.

Availability allows a legitimate user to access confidential information after it has been properly authenticated. When availability is compromised, access may even be denied to legitimate users due to malicious activity such as denial-of-service (DoS) attacks.

Integrity implies the unauthorized modification of information. This could also mean changes to information while the same is in transit in space or while it is being stored on some type of support. To protect the integrity of information, efficient

techniques for validation must be implemented. These techniques can be integrity checks or digital signatures.

The threats facing banks and AIS may classified to, internal threats and external threats. The internal threats emanates from someone working inside the banks, whereas the external threats emanates from an outside person (Okpamen, 2013:7):

1-Internal threats:

False Accounts: The bank authorities might open false accounts in the names of fictitious customers and allow privileges to that account. They may provide such accounts with loans and credits. Later, they might convert this money to personal use.

Fraudulent loans: One of the way to take off cash from the bank is to bring out a loan. A fraudulent loan is one way that the owner (borrower) of a business entity dishonest person work for a bank or a helpmate; “the burrower” could then report bankruptcy or disappear. Finally, the cash is lost. The borrower might even be a non-existing entity and the loan just a trick to hide a steal of a big sum of cash from the bank.

Wire fraud: Wire transfer networks such as the universal SWIFT interbank fund transfer are always is the aims because if a transfer done, it is hard or out of the questions to inverse. Because these networks used by banks to disband accounts with each other, fast or overnight wire transfer of big amounts of cash are familiar; while banks have placed checks and balances in place. The insiders may create risks by trying to use fraudulent or false documents, which demand to demand a bank depositor’s cash be wired to another bank, always account in some distant foreign country.

Forged or fraudulent documents: false documents are always used to hide other robberies. Banks tend to count their cash accurately, so every mite must be count for. A document claiming that a sum of cash has been borrowed as a loan, outgoing by an someone (depositor) or transferred or invested, can thus be worthy to a banker who desire to hide the small detail, and suppose that the cash has been rubbed and now is lost.

Theft of Identity: Dishonest bank employee have been known to disclose depositor’s personal information to use this information in identity theft frauds. The perpetrators then use the information to obtain identity cards and credit cards, using the victim’s name and personal information.

Demand Draft Fraud: This fraud is usually done by one or more of the bank’s dishonest employees. They remove few demand draft (DD) let go or DD records from paper and write them like a usual DD. Since they are employees, they know the coding and making of a demand draft. These Demand Drafts will be issued payable at a distant town/city without debiting an account, and will be cashed in payable section. For the paying branch, it is just another Demand Draft. This kind of fraud will

be discovered only when the chief office does the section- wise fittings, which usually takes 6 months. By that time, the money is unrecoverable.

2-External threats:

These are the threats from outsiders, and can be done by thefts or hackers. Someone using the internet banking for transactions has to be careful of hackers. The security number and password are vital information for your online transaction some of these threats listed below (Okpamen, 2013:8):

Credit card Fraud: Typically, the fraudster uses the credit card of another person to be charged for the purchase. Some of the credit card frauds are stolen card frauds, Account Takeover Fraud, Credit Card Mail Order Fraud, and Skimming.

Stolen Credit card fraud*:* When a customer losses a card it is possible for the thief to make unauthorized payments on the card until the card is cancelled.

Account Takeover Fraud: Fraudsters call and impersonate actual cardholders using their stolen personal information. They have the address and other information of the cardholder changed to an address they control. Additional cards and possibly PIN mailers are requested and issued to the new address and used by the fraudsters to make purchases or obtain cash advances.

Credit Card Mail Order Fraud: Using a stolen credit card number, or computer generated number, a thief will order stolen goods.

Skimming: Skimming is the theft of credit card and information by a dishonest employee; it is usually done at bars or restaurants. Those people either copy the numbers manually or they use a magnetic stripe reader to get the card security code.

Phishing or fraudulent mail: Phishing is a fraud technique used to make people to give their security numbers and password to fraudsters. The hacker sends a fraudulent mail, which is specifically designed to reveal the security details to the intended person. This mail is designed in such a way that it looks like it has come from a responsible source e.g.; your bank. This mail might also provide you with a hyperlink with your bank home address URL that is again a fraud site. You might find this fake site exactly same as the original one where you can easily end up giving your security details to the hacker or fraudster. How phishing could be avoided is listed below:

First, no bank will ever send a mail asking about your security number and password. If you do receive a mail from your bank, no matter how urgent it is never ever put security information on it. Always call the bank phone number to verify whether they want this information. Secondly, if you suspect that it is a fraud mail forward it to the bank reporting about this fraud.

Check the security Bank sites: You should never click on a hyperlink or follow a link to go to your bank home address on internet. Always type the whole address of your bank URL in the browser. Check whether the bank site starts with ‘https’ and whether there is a padlock icon at the bottom section of your browser. When you

double click on the padlock icon it brings the information about the lock, which will help, you confirm whether this site is genuine. If the lock is not valid or has been issued to a website that you do not recognize, do not enter your security information.

Login and Logout: Do not provide your security ID and password to anyone to avoid frauds. Do not leave your computer or laptop unattended while you are still logged into your internet banking. Always logout when the session is over. Avoid saving the security ID and password on your computer and always keep it in a safe place. Also, do not change your security details when you are using a computer in a public place.

5- Modern Security Applications in Banks and Accounting Information Systems (AIS)

One of the biggest exposures for many computer systems today is the software running on it. Whether this software is the operating system, a service provided by the OS, an application, or database, efforts must be taken to prevent system vulnerabilities and compromise. The following sections outline the minimum steps for protecting the "core" software components of AIS and banks systems (Zimmerman, 2016:7):

Operating System Hardening and Patching: Operating Systems are loaded by the Systems Engineering Mid-Tier Infrastructure or Desktop Support groups and follow a standard procedure that includes evolving best practice and integration of appropriate patches and Hotfixes identified by Mid-Tier, the Information Security Officer and SOS.

Existing systems shall receive updates on a periodic basis as determined by the MTI, Database and LAN/Desktop Groups. Any update determined to be of a "Critical" nature

shall be applied to systems within a week after it is release from the vendor. The MTI, Database and LAN/Desktop Groups are responsible for ensuring that testing of patches is performed prior to installation. On desktop systems, the installation of these updates shall be automated where possible.

Authentication Standards: All user authentication for restricted access is accomplished by the use of WebAccess filters, 2-Factor authentication (as directed by AIS management) or by confirming user ID and password combinations against the ITS centrally managed user account repository. Authorization is performed in conjunction with group definitions in the ITS LDAP repository where possible. If LDAP authorization is not possible, authorization methods may occur through the OS, Database, or application level security.

Application Hardening: For applications that have been developed external to the organization, Penn State employees responsible for supporting the applications must keep AIS support staff aware of security-related updates. Implementation of such updates shall be coordinated with the MTI group.

Application and Web Application Vulnerability Scans: All applications hosted within AIS will be initially scanned for vulnerabilities and Web application (if applicable) issues for vulnerabilities prior to initial deployment. Continuing periodic scans must be performed thereafter on systems in Production environments. All servers shall use encryption and cipher suites approved by the AIS Information Security Officer and Senior Director.

Firewalls: A firewall is the first line of defense against hackers. It is a computer program that is installed on a computer that connects a network to the Internet. The firewall analyses the packets that pass in and out of the network. It is programmed to follow certain rules, which enable it to decide whether or not to allow a packet to pass. There is firewall software that can be installed on a stand-alone PC.

Access rights: Access rights can refer to both physical and software. In a physical sense, these refer to different members of staff who have to gain physical access to certain areas. For example, access to the room containing the mainframe may be restricted to operators. Software rights refer to the level of access different users have to different levels of data and information.

Password policies: Password policies refer to guidelines or requirements on the structure and use of passwords. They can be required for access to a computer system or a group of files or a single file.

Data encryption: Data should be encrypted. Encryption scrambles the data and makes it unintelligible without the use of a key. The key is used to decipher the data.

Anti-virus software: Anti-virus software scans files for pieces of code, called signatures, which it recognizes as part of a virus. Updating anti-virus software mostly involves updating the signatures file. This should be done on as frequent as basis as possible. This is even more the case when you receive files regularly from outside sources. The actual anti-virus program itself will be updated from time to time. These updates will include additional features and improved methods of scanning. It is important to keep in mind that no anti-virus software is perfect. It is only as good as the techniques it uses for detecting viruses and the currency of the signature file. There is always the

Chance that a virus will go undetected. However, a good anti-virus system installed on your system is essential and will usually detect most viruses. When a virus is detected, the software will attempt to remove the virus. This is called cleaning or disinfecting. It sometimes happens that the system can detect the virus but not get rid of it. In this case, you will usually be given the option of deleting or quarantining the infected file. When a file is quarantined, it is made unusable and so unable to spread the virus. A future update of the software may be able to remove the virus. If it can the quarantine is removed.

Staff employment practices: Basic to good company security are loyal and trustworthy staff. If staff are likely to have access to sensitive information, they should be thoroughly screened before they are employed. The more sensitive the

information they have access to, the more vital is this process. Promotion to more sensitive positions can be based on a good history or loyalty and trust. Part of the staff induction process and on-going staff training should inculcate in staff the importance of security and an awareness of the consequences of its violation.

Security procedures: Information should be classified on the basis of its sensitivity. Access rights to this information should be limited to those who need to know. To access certain information, an employee might need a special security clearance. All access to sensitive information should be recorded. The question of access rights is discussed further in the next section. Where sensitive information is stored in the form of paper files, these should be kept in a secure vault. Procedures should be in place that enable staff to report breaches or suspected breaches of security. They should be able to report these without fear of reprisal. In large organizations, security departments can be established specifically for the purpose of providing. Such channels and monitoring security on an on-going basis. This is often done in conjunction with forensic auditing. This is a special form of auditing to detect mismanagement and corruption.

6- Data analyses

Description of personal factors and functional respondents: Table 1 shows a description of personal and functional factors of the sample individuals, as follows:

- Gender: it is shown that 35 % of the sample is male, and 65% is female.
- Age range: it is shown that 27.5% of the sample their age from 25 to 30 years and 40% between 31- 40 years, 15% between 41 to 50, and 10% between 51- 60 years, 7.5 % of that above 60 years.
- Education: 87.5% of the sample research has Bachelor degree, and 7.5% of the sample has Master Degree and 5% of the sample has PHD degree.
- Specialization: shows that 35% of sample is accounting specialization, 27.5% of respondents are business administration specialization, and 30% are finance and banking specialization, 5%, of them are economic and 2.5% from other specialty.
- Experience years: 17.5% of the samples study their experience less than 3 years, 22.5% less than 5 years, 32.5% less than 10 years and 27.5% more than 10 years.

Table 1. The frequencies and percentages of the personal levels of the respondents

Factor	Details	Frequency	Percentage %
Gender	Male	14	35
	Female	26	65
Age range	25-30 years	11	27.5
	31-40 years	16	40
	41-50 years	6	15
	51-60 years	4	10
	Above 60	3	7.5
Education	BS.c degree	35	87.5
	MS.c degree	3	7.5
	PH.D degree	2	5
Specialization	Accounting	14	35
	Business administration	11	27.5
	Finance and banking	12	30
	Economy	2	5
	Other	1	2.5
Experience years	Less than 3 years	7	17.5
	Less than 5 years	9	22.5
	Less than 10 years	13	32.5
	More than 10 years	11	27.5

7- Hypothesis testing and results of the analysis

Below is Table 2 shows the arithmetic mean, standard deviation, and the uses of modern security applications in banks and AIS, which reflects positively on banks and AIS particularly:

Table 2. shows the arithmetic mean, standard deviation, and the uses of modern security applications in banks and AIS, which reflects positively on banks and AIS particularly

No.	Paragraph	Arithmetic mean	Standard deviation	%	Ranks
1	Bank uses modern security methods in accounting information systems planning	4.24	0.67	84.8	1
2	Bank uses modern security methods in accounting information systems security	4.09	0.72	81.8	5
3	Bank employs modern security methods to monitor the performance of accounting information systems	4.11	0.69	82.2	3
4	Bank uses modern methods security to develop accounting information systems applied in it	4.04	0.89	80.8	9
5	Bank has good accounting information systems security training program for its computer users.	4.06	0.91	81.2	8
6	Bank has modern accounting information systems provide good credit protection through the identification of appropriate ceiling for credit	4.08	0.68	81.6	6
7	You has good of the bank's accounting information systems security program	3.84	1.07	76.8	11
8	The most attacks on banks and accounting information systems is computer virus attacks	4.10	0.85	82	4
9	The most attacks on banks and accounting information systems is through direct manipulation attacks	4.07	0.78	81.4	7
10	The most attacks on banks and accounting information systems is unauthorized access attacks	4.01	0.84	80.2	10
11	Banks and accounting information systems has lacks as systems	4.14	0.83	82.8	2
12	Training on Modern Security Applications enough to get required knowledge	3.58	0.94	71.6	12
	Total	4.03	0.82	80.6	

8- Results:

The research found the following results:

1. Banks use modern security applications methods in accounting information systems.
2. 2- There are difficulties in the use of information systems, accounting, or part of it.
3. 3- There are difficulties in the use of modern security applications methods or part of it.
4. There is lack in accounting information systems used by banks.
5. The training periods and methods are not enough for the employees to provide them with required knowledge about modern security applications.

9- Recommendations

The research recommends the following:

1. The research recommends improving use of modern security applications methods in banks and accounting information systems.
2. Put more efforts to overcome difficulty of using information systems, accounting and modern security applications methods.
3. Work on the development of accounting information systems to fix the lack problem and then preventing for banks futures.
4. Banks needs to increase training strength and period in all directions in accounting information systems to provide required knowledge about modern security applications and then minimize possible threats that may appears.
5. The research recommended further researches on the role of modern security methods in accounting information systems in investment decision, credit decision and future customer's services.

References

1- Bawaheh, Shamsi S., **Information security for Organizations and Accounting Information Systems:** A Jordan Banking Sector Case, International Review of Management and Business Research, Vol. 3 Issue.2 June: 1174-1188, 2014.

2- Garzia, F., **Handbook of Communications Security**, WIT Press Southampton, Boston: 449, 2013.

3- Goreva, Natalya, Luther, Elaine and Bromall, George, **Exploring Accounting Information Systems and Embezzlement from Nonprofit Originations**, Issues in Information Systems, Volume 14, Issue 2: 39-46, 2013.

4- Hall, James A., **Accounting Information Systems**, South-Western Cengage Learning, Seventh Edition: 7, 2011.

5- Muhrtala, Tijani Oladipupo and Ogundeji, Mathias, **Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies**: The Nigerian Case, Universal Journal of Accounting and Finance 1(1): 9-18, 2013.

6- Neogy, Taposh Kumar, **Evaluation of Efficiency of Accounting Information Systems: A Study on Mobile Telecommunication Companies in Bangladesh**, Global Disclosure of Economics and Business, Volume 3, No 1: 40-55, 2014.

7- Okpamen, Peter, **Security of Information Systems in Organization: A Bank Model,** Mediterranean Journal of Social Sciences, Published by MCSER-CEMAS-Sapienza University of Rome, Vol 4 No 7:7-8, 2013

8- Kieso, Donald E., Weygandt, Jerry J. and Warfield, Terry D., **Intermediate Accounting**, John Wiley & Sons, Inc., Fifteenth Edition: 84, 2013.

9- Spiceland, J. David, Sepe, James F., Nelson, Mark W. and Thomas, Wayne B., **Intermediate Accounting**, McGraw-Hill Education, Eighth Edition: 52, 2016.

10- Varley, David, **Concepts of Information Technology**, Published by the ICDL Foundation, ICDL Module 1: 55-56, 2006.

11- Zimmerman, Mark, **AIS Acceptable Use and Information Security Procedures**, the Pennsylvania State University, 2016.

تطبيقات الحماية الحديثة في المصارف ونظم المعلومات المحاسبية

م. محمد قاسم شيرزا

المستخلص

ان انتشار الانترنيت قد غير بشكل كامل تعريف طبيعة امنية المعلومات وجعل جميع الشركات بصورة عامة والمصارف بشكل خاصة تواجه تهديدات عالمية لشبكاتها بل ان الأهم من ذلك هو ان البيانات والمعلومات المحاسبية في مواجه لهذه التهديدات. فقد ارتفعت اعداد الحوادث الأمنية للأنترنيت كل عام عن العام الذي سبقه وعليه فان الحقائق السابقة الذكر أدت الى هذا البحث.

وهدف هذا البحث الى تقييم تطبيقات الحماية الحديثة في المصارف ونظم المعلومات المحاسبية وللوصول الى هذا الهدف تم الاستعانة باستبانة ذات أسئلة متعددة.

ولقد توصل البحث الى عدة نتائج كان من اهمها ان المصارف تستخدم تطبيقات الحماية الحديثة وان المصارف تواجه فقدان (نقص) في نظم المعلومات المحاسبية.

ولقد خرج هذا البحث بتوصيات عديدة كان من اهمها ضرورة زيادة التركيز على التدريب في جميع جوانب نظم المعلومات المحاسبية للحد من التهديدات المحتمل ظهورها.

* كلية المنصور الجامعة