PROTECTION OF THE INFORMATION SYSTEMS IN THE BANKING SECTOR

Thomas Chatzigagios*, Doranis Ilarion

University of Macedonia, Thessaloniki, 54006, Greece

Abstract

The arrival of computers has led to the creation of Information Systems which are being used as a business tool extensively. Computers and more specifically information systems are used in a large scale from almost every single enterprise. The application of the dynamic potential of information systems and technologies has brought various improvements in business activities.

One of the most important sectors which takes advantage of the constant rise of informational systems are the banking institutions. The nature of the banking sector as in other industries related to financial institutions, includes the use of terms such as information and trust. As a fundamental part of the industry of services, banks need the most information they can acquire.

In the financial level, the role of an information system is far more complex, due to its position in the chain value, where the need for advanced information systems, which will allow the function of a large volume of information in different stages of processing, is granted. Furthermore, for the banking institutions and their clients, it is indispensable to have security, accuracy and data availability, terms which contribute to the automation of Information Systems.

The basic services include the recordings of client's audit books, whereas the most complicated include the possibility of an interactive voice recording through which clients can receive answers through the frequently asked questions application. However, the development of an information system requires substantial investments, the responsibility of not leaking information and different other security measures. Therefore, banks need information in every stage of their activities. The benefits of information are many. Today, the decision making systems are used also by banks for purposes of commercial use of new loans. Typically, banks tend to need information in several levels analyzed in the paper.

Keywords: *banks, bank security, information systems*

1. INTRODUCTION

The objective of this paper is to present the measures for the protection of banking and information systems. The development and evolution of computers has led to the creation of Information Systems which are being used from the personal level, to businesses, to organizations, to whole countries. In the business sector, information systems are used by almost every single enterprise as a business tool in a large scale. Computers and more specifically Information Systems are used in a large scale from almost every single enterprise. The application of the dynamic potential of information systems and technologies has brought various improvements in business activities in terms of production, financial management, accounting, organizing clients and suppliers etc. One of the most important business which takes advantage of the constant rise of technology in informational systems are the banking institutions. The nature of the banking sector and more general financial institutions, includes the use of terms such as information and trust. In this sector, a huge amount of information is processed all the time.

Furthermore, for the banking institutions and their clients, it is indispensable to have security, accuracy and data availability, terms which contribute to the automation of information systems.

The banking institutions have as their object investments, commercial and depository activities amongst which are the following: the attraction of financial assets from the public and the appropriate financial carriers with the form of depositions, granting loans, payments and transactions in a foreign currency, transaction activities such as the exchange of coins, and offers in a foreign currency. The

information system of banking institutions has to assure the execution of these specific activities, but also has to fulfill some basic requirements.

As an indispensable ingredient of the sector of services, banks need to store information in order to improve the level of their services and to acquire a competitive advantage in regard to their competitors. More specifically, new technologies such as cloud computing and other storing systems of data which are based on the internet, have allowed to the banking institutions to grant their clients state of the art services, preserving however the competition of the financial market which is required during the practice of their business activities.

The basic services include the recordings of client's audit books, whereas the most complicated include the possibility of an Interactive Voice Recording through which clients can receive answers through the frequently asked questions application. However, the development of an Information System requires substantial investments, the responsibility of not leaking information and different other security measures. Therefore, banks need information in every stage of their activities. The benefits of information are many: Today, the decision-making systems, are used also from banks for purposes of analyzing the credit history and credibility of every applicant (individual or business) before granting them new loans. Typically, banks tend to need information in the following levels:

Basic level 1:

This is the most basic level. Information in this level can only be used for administrative purposes. Their duties include book registrations, using of customer accounts. The revolution of banking through the Internet has transformed the basic level into something much more attractive to the customers than what it used to be. In addition, the notion of telephone banking through Interactive Voice Recording has proven that it is an important technological pace to the benefit of Banking Institutions and Information Systems.

Advanced level or level 2:

In this level, information is something critical and is used at a managerial level. Managers use specific information such as list of stocks and annual meetings in databases which are supposed to be safe. This level of information is supposed to be secured and cannot be distributed without prior consent and proper authorization. Information at this level is difficult to be used by clients. However, in extreme cases of fraud and deception, banks can use this kind of information as a security measure to ensure that their reputation will not be at stake and in anyway be damaged.

In our time, almost for all the procedures which a bank tries to fulfill, informational systems are used. The queues which were forming in the near past have begun to diminish as banks work online the biggest part of their applications. For the use of online applications, it is required apart from connecting to a central computer, the gathering and processing in a local level, which is a branch level, a transfer file in the beginning or in the end of a day.

1.1. Appraisal of protection in banking information systems

All the banks in western countries and more recently in Asian countries use Information Systems in order to exist and operate in the global markets. The tools of decision making, administration systems of accounts and systems which are based upon the internet are being widely used from banking institutions in order to operate regularly and attract new customers by being ahead of their competitors. However, the main problem of on-line applications which they provide is the level of security. Security constitutes an essential requirement for the ensuring of normal functionality of a banking institution. By nature, it does constitute a dynamic and not static parameter and subsequently will have to be constantly reexamined and reevaluated with the goal of improvement. With the term "security of banking information systems" we mean the ability of a banking institution to provide reliable and trustworthy information which can also be accessed by anyone interested anytime.

In order to accomplish this goal, protection of integrity and confidentiality of data is required as well for the constant operation of an information system center.

Furthermore, the safety of banking information systems is divided in two major categories:

1) Safety in emergency cases
2) Safety in everyday transactions

2.1. Safety in emergency cases

Safety in emergency cases usually incudes cases of malfunctioning of an information center from power failures, temporary shortcuts from fire, loss of communication lines and failure of a part of the equipment or the main computer system. In order to deal with such situations, usually there is a transfer from the main to the auxiliary system which is implemented in most of the banks. Sometimes it is also common for the banking institutions to stop their operation until the problem has been resolved and the full capacity of the system has been returned.

2.2. Safety in everyday transactions

The most common threat for on line users of banking applications is the theft of security codes (pin) and their electronic cards or the theft of usernames and private banking accounts passwords and subsequently the loss of money. The truth is that there is no perfect system. Every system has its weakness as it includes programming and decoding. However, recently many banks have taken precautionary measures so as to have secure online banking transactions through the use of computers and Information Systems. The new security systems include the Secure Sockets Layer (SSL) technology as well as systems of memory which use access codes. Furthermore, the providing of extra information as well as the providing of access codes in specific telephone numbers is planned. As regards internet banking, this makes available all the security issues for its application and for its transactions as for example authentication through a multichannel personal identification number (PIN), random generated positions from the system for every connection, daily maximum limits for everyday transactions.

More specifically, safety in everyday base of banking transactions can be implemented initially through the natural security of banking Information Systems. If, however, the right measures will not be taken properly, there is the danger of malfunction or even destruction of hardware and subsequently loss of vital information.

Furthermore, the safety of Information Systems has to be ensured through the development of mechanisms: protection of memory, file accessing and back-up safety copies known as back-up systems. In addition, it would be good to develop systems of continuous operation, anti-virus programs and log entries where there will be a recording of all the changes which are related to the operation and security of an Information System (logs). Network and equipment security transactions can be accomplished through the creation of passwords, accessing boards, smart cards, whereas the protection of messages which are transmitted via the Internet with the use of modern methods of cryptography as well as other methods of authenticity and verification.

In conclusion, security of other networks, peripheral and auxiliary equipment can be accomplished through the systematic taking of back-up copy measures, use of accessing controls or security packages, implementation and use of anti-virus programs, education of users in protection techniques, saving of confidential files in a secure place and the physical protection of the personals' computer place, of the peripheral and auxiliary devices. Special care must be given to the Banking Institutions' Information Centre from attacks by malign software or viruses which could infect terminals and provoke the leaking of vital banking data in favor of hackers

2.3. Interception

Interception constitutes a form of passive attack against the confidentiality of Information Systems from a person (hacker) or a program or a mother computer system. The accumulation of a large quantity of electronic information regarding individuals from banking institutions, public services and private enterprises in conjunction to the ability of computers to survey and total recording of information for individuals, creates in our modern time period, an increasing threat to private life. In addition, the protection of private life, of personal data and in particular of sensitive private data is considered very important and significant for every person (individual or organization). The term

"personal data" includes every piece of information which describes a person like the name, the surname, the profession, the marital status.

When we refer to the term "interception", we mean the interception of personal data under its distribution in the internet. People who have access to information must also have an access authorization. It is understood, that the interception of information can potentially create dangers not only to a personal level, but also to a financial, business and even on a state level by intercepting data regarding to the national security. Specifically, interception constitutes an act of deceit of a user with the intent to give personal information like his address, the number of his id, or the number of his passport or even the number of his bank accounts to a fake internet page. Through this procedure, it is possible for a hacker to steal or photograph personal data of a user and to acquire illegal access to his personal data like emails, secret passwords, bank accounts for nefarious purposes. Due to their specialized knowledge in Information Systems, hackers can "brake" codes and enter into computer systems jeopardizing the protection of private life and the integrity of data before they can be perceptible from a security system. The amount of information they collect, they either use for their own sake or they disclose it to other parties in exchange of money. The buyers of this kind of information, for example, use techniques to locate credit cards who have the highest credit limits or the highest remainders. Usually, they seek out specific account codes which signify that a certain ban account has been created many years ago as the most customers have probably higher credit limits.

It is also important that the disclosure of personal data which are registered in an Information System violates the legal frame regarding the protection of personal right of individuals and can be prosecuted legally.

The most important problem is located basically in the traditional email messages as electronic messages can be monitored easily and can be subsequently used in favor of criminal activity. Having some basic information regarding a user of email, a hacker can acquire a freeware software program in the internet which will allow him to monitor the email of any user. As soon as the surveillance of an electronic message takes place, a hacker can intervene in the communication through email with four different ways. These are the following:

a) Eavesdropping attacks, during which information remains intact but the private life of a user is violated.

b) Tampering, during which a hacker changes the content of an electronic email message and then sends it to its receiver.

c) Spoofing, under which a hacker pretends that he is the legal owner of an email.

d) Misrepresentation under which a hacker orders data using a credit card and specifically uses the cards' security passwords and pins, which he has previously intercepted from its rightful owner.

2.4. Techniques of dealing with Interceptions

The rapid development of technology in the field of computer systems and the transmission of information has demonstrated an important problem, the one of protection of the transmitted information and subsequently that of the privacy of users. The basic technique used in order to eradicate the problem of interception is that of cryptography. This method is very easy in its application, follows typical protocols and keys of cryptography and provides solid protection of data. For these reasons it is preferred. Its goal is to ensure the integrity, authentication and confidentiality of data during their transfer between the sender and the receiver via the internet. More specifically, the data which are going to be shared are transformed in such a form that it is difficult to be interpreted and read if a certain sequence is not known. This sequence is the key to solving encrypted data, in conjunction with the use of a suitable algorithm. In order for someone to be able to obtain access in specific data, he has to know the key. In our time, cryptography techniques offer data encryption in application levels during their transfer between two computer terminals which communicate through the Internet.

The modern cryptography techniques are necessary to every Information System which requires to store personal data. However, we have to highlight that cryptography does not provide by itself protection from data infringement except in the case when it is applied properly in a specific frame. Only in this way it can be considered as a "fence" around personal data.

The second technique used is the filtering of access codes. Today, the modern procedures of filtering codes of access control the users' selected code by prearranged criteria established by the policy of safety. For example, a security code must include at least one arithmetic and one alphabetic character, cannot belong to a well-known list of passwords and cannot be connected to a personal information which the user has already had introduced to the Information System. It is important that in high-security systems, the procedures of checking the users' codes include similar techniques to the ones used by invaders of information systems. A special software program is used in these cases to check the code of access a user has chosen.

Another technique which is used is the parametrization of operating information systems. In elder systems, the password file was located in a catalogue and was identifiable from all users of the system. The invader had the possibility to copy the file and the codes and subsequently to launch a "dictionary attack". In modern systems, the specific files are accessible only to the administrator of the system. For this reason, these systems are called "shadow systems".

The Intrusion Detection System (IDS) which is applied in the Information System is programmed to lock automatically the users' account in case of an on-line attack by an intruder. Despite the fact that this specific policy is not the most effective, especially in cases of attempting to retrieve money from ATMs with stolen cards, it should be used with extreme circumspection, because it often leads to the so-called denial of service attacks where the invader attempts to enter the system with the aim of locking one or more accounts.

Finally, we have the policy of codes renewal. The imposing of renewing the codes in regular time intervals, limits the problem of interceptions, without however totally eliminating it. In order to be able to steal personal card data, many internet sites offer attractive offers. In this way they urge the users to register their personal data cards. Then, they use these data to charge their cards in other websites. In websites where the users' card data are saved, there is a high probability for these data to be stolen. This is the reason that sensitive data should not be saved and strict measures should be implemented for their safe maintenance. If an interception is known, then institutions notify the corresponding banks which also notify their clients to revoke their cards and issue new in their place.

3. REVIEW OF LITERATURE

The topic of protection of information systems in the banking sector is important and topical. Many articles and books have been published on this subject. The most important are those of Davenport and Laudon.

4. SUMMARY AND CONCLUDING REMARKS

In conclusion, we examined in this paper the importance of the matter of protecting the sensitive personal data in the Banking Information Systems. This topic is especially vital to the majority of users throughout the world. As technology rapidly advances, new methods of attempting to retrieve personal sensitive data from cards and accounts are introduced. In the same way, new counter measures are also appearing. We can conclude by expressing the belief that there does not exist a totally protected Information System in the Banking sector or in any other sector. However, through the process of experimentation and improvement on the existing systems, we may come to the point where it will be extremely difficult for a potential hacker to acquire access to the personal accounts of different users. Further research is focusing on inserting personal biometric characteristics of an individual in order to have access to his personal data. In this way it will be very difficult for a

potential hacker to invade the accounts of users because the biometric characteristics of every individual are unique.

REFERENCES

1. Adeoye, O.S. 2012, "Evaluating the Performance of Two-Factor Authentication Solution" in *The Banking Sector, International Journal of Computer Science Issues*, vol. 9, is. 4, no.2, pp.457-462
2. Baker, R. 1991, *Computer Security Handbook*: TAB Professional and Reference Books.
3. Back, A., Möller, U. & Stiglic, A. 2001, "Traffic analysis attacks and trade-offs in anonymity providing systems*"*, in *Information Hiding*, Berlin: Springer, pp. 245–257.
4. Baxter A. 2015, *How to stop hackers from stealing your information on public Wi-Fi.* (Retrieved in 23.09.2017). Retrieved from https://thenextweb.com/insider/2015/08/08/how-to-stop-hackers-from-stealing-your-information-on-public-wi-fi/#.tnw_kXzFhIAJ
5. Dai, H.-N., Wang, Q., Li, D. & Chi-Wing Wong, R. 2013, "Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas", *International Journal of Distributed Sensor Networks*, vol. 2013, no. ID 760834, pp. 1-13
6. Davenport, T. & Short, J. 1990, "Information technology and business process design*", Operations Management*, Vol.3, pp.11-27.
7. Laudon, K., & Laudon, P. J. 2012, *Management Information Systems* (12 ed.).