"Dimitrie Cantemir" Christian University
Knowledge Horizons - Economics
Volume 6, No. 1, pp. 122–125
P-ISSN: 2069-0932, E-ISSN: 2066-1061

www.orizonturi.ucdc.ro

MANAGEMENT OF INFORMATION SECURITY IN FINANCIAL ACCOUNTING

Aurel ŞERB[1], Constantin BARON[2], Nicoleta Magdalena IACOB[3], Costinela-Luminiţa DEFTA[4]

[1,3]*Faculty of Finance, Banking and Accounting Bucharest, "Dimitrie Cantemir" Christian University, [1]E-mail: aurelserb@yahoo.com,*
[3]E-mail: nicoleta.iacob_2007@yahoo.com
[2]Faculty of Marketing, Bucharest, "Dimitrie Cantemir" Christian University, [2]E-mail: constantin_baron@yahoo.com
[4]Faculty of Tourism and Commercial Management, "Dimitrie Cantemir" Christian University, [4]E-mail: lumi.defta@yahoo.com

Abstract *Security issues in financial accounting are complex, and the risks are often difficult to stipulate, even for experts. The issues presented in this article try to be formed in a contribution to the consolidation of problems in the field of risk, and former vulnerabilities in cyber security in financial accounting. The use of an information security management system became a requirement for organizations because on the states began adopting mandatory data protection legislation and information, but also because of attacks on organizations that may have severe negative consequences such as stealing and selling confidential strategies by competitors, branch and technological secrets, theft and using for illegal purposes of customer data etc.*

Key words:
Cyber security, vulnerability, threat and risk, information security management systems

JEL Codes:

1. Introduction

Many users, not only from financial accounting, are still not aware of the possible vulnerabilities, threats and risks they meet by using computers, software and software application and communication networks or solutions that already exist to make them face. Security issues are complex, and the risks are often difficult to stipulate, even for experts. Lack of information is one of the imperfections of the market, on which security policies should be to have in mind. There is a risk that some users alarmed of so many reports and threats to security, to avoid simply the use some of the information systems. Others, which are either not scripturally informed, or underestimate the risk, may be too negligent. Paradoxically, there is an impressive quantity of information in the field of computers, networks and security of the information available on the Internet and magazines about computers covers the subject quite well. The issues presented in this article try to be formed in a contribution to the consolidation of problems in the field of risk, and former vulnerabilities in cyber security in financial accounting.

2. The Definition of Informatics Security[1]

Informatics security could be defined, generally speaking, as a complex of procedural, physical, logical and legal measures that intended to prevent, detect, and correct various categories of "accidents", either as they originate from natural causes, or as they appear as a result of acts of sabotage. By categories of accidents are understood those accidents that endanger human life, material assets, information, and values, not in the last of all, the surrounding environment. From the perspectives of this possible definition arise as informatics security may be structured on three levels, as follows:

1. *Physical security* is the "outside" of the information security and consists in the prevention, detection and limiting access directly on the goods, values and information. The important problem in financial accounting area is that of saving spare copies of data and programs, and secures storage of these carriers. In this context local networks are a great help; reliable persons may save the data directly on the server that you deposited. In distributed systems first measure physical security assurance is to prevent access to equipment, this being actually valid for all systems, either as they are distributed or not.
2. *Logical security* represents all methods which ensure the control of access to resources and system services. Logical security has several levels, which in fact can be divided into two levels: levels of network security access (NSA) and levels of network security services (NSS).

Levels of network security access consist in availability to check, verify, and set the access rights of users.

[1]Şerb A. (2010). *Securitate informatică*, Editura Pro Universitaria, București.

Highest level of security of access is the level of access to the system. At this level can be determined if and when the network is accessible to all users, groups of users, or only to the individual stations. It also may be liable to uncouple a station, and access management. Behind the level of access to the system is the level of access to the account. This level checks if the user who connects with a specific name and password exist and is a valid user profile. The innermost level in the security access levels is the level of access rights. After it has gone through the level of access to the system and the level of access to the account, the level of access rights determine privileges envisaged by the user. Some of the functions that can be implemented with levels of security access refers to the provision of accounts (for connection time, use the disc, etc.) and the management of evident user access.

Levels of services security control the access to the services system, such as wires tunes, inputs/outputs to the disk, server management, etc. Highest level of services security is the level of services control, which is responsible for the functions of warning and reporting services whit. Also, it enables and disables certain services. After the level control of services has established a service, the level of rights of services determine exactly how to use a specific service account given. Also the level of rights of specific services manages rights. If it is an account of a member or of one or more groups, then the level of rights of services will ensure that this account will inherit rights of the group. You can include high level services and specific software (SIS), as well as low level services specific hardware (SSH). SISs are operations which are not limited hardware – for example, the request to open a file without a name. Other services are access to queues and the email. SISs are actually constructed via SSH and may require more low level functions to run. SSHs are dependent on the hardware. These services are "bricks that are" fundamental to the construction of the system and they cover the levels of inputs/outputs for the other levels.

3. *Legal security* is the level composed from a collection of national and international laws governing act of violation of security levels to physics and logic and establishes criminal sanctions for these acts.

3. Concepts of Vulnerability, Threat and Risk

Vulnerability is a flaw or weakness in the design or implementation of hardware, software, networks, or computer-based systems, including security procedures and controls associated with the systems[2]. Vulnerability can be exploited, intentionally or unintentionally, in order to affect adversely the goods and the activities of a person or organization. The vulnerability is a weakness of the system so that allows an unauthorized action.

A threat is any circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a system, resulting in a loss of confidentiality, integrity, or availability. Threats are implemented by threat agents. Examples of threat agents are malicious hackers, organized crime, terrorists, and nation states[3].

Risk is a combination of the likelihood that a particular vulnerability in an organization`s systems will be either intentionally or unintentionally exploited by a particular threat agent and the magnitude of the potential harm to the organization`s operations, assets, or personnel that could result from the loss of confidentiality, integrity, or availability[4].

4. Classes of Vulnerabilities, Threats and Risks

The literature offers different ways of classifying **v**ulnerabilities, threats, and risks. These classifications can be made having in mind various criteria. Some of the most important **v**ulnerabilities, threats, and risks that are affecting financial accounting area will be presented in the following items.

• *Wiretapping, Eavesdropping on Emanations* - can be achieved through a variety of methods, such as telephone or radio surveillance ties, exploiting the electromagnetic radiations issued, routing data through additional knots less protected.

• *Intercepting the information entered from the keyboard* – can be achieved by recording sounds produced by the keyboard to be used to decipher the text written by the user.

• *Scanning* – the activity by which certain programs or technical means can be automatically monitored certain types of activities performed on a computer, or in a network of computers.

• *IP sniffing* – this type of attack consists in monitoring information that circulates through a network interface to detect information transmitted in unencrypted mode through the network (for example, IP addresses, or passwords). Programs which perform network traffic interception are called sniffers.

[2] Interagency Working Group on Cyber Security and Information Assurance, S.U.A. (2006). *Federal Plan for Cyber Security and Information Assurance Research and Development*.

[3] Interagency Working Group on Cyber Security and Information Assurance, S.U.A., op.cit.

[4] Interagency Working Group on Cyber Security and Information Assurance, S.U.A., op.cit.

• *Password sniffing* – are programs that test automatically the password, by making step-by-step an attempt with each word from the dictionary, ending what is found on the password used.
• *E-mail spoofing* – these attacks acts trying to steal the address used by the Internet Protocol when is accomplished a connection in a network, and spoofing the sender's email address (E-mail spoofing).
• *Harassment* – usually can take place when a threat enjoys himself by exploring his possibilities in the field of exploiting coding by, or/and capabilities offered by the computer, or when threat agents (known under the name of spammers) transmit enormous amounts of email (or other kind of information), as unsolicited offers, or random information, things submitted in order to block certain servers.
• *Session hijacking* – the threat agent finds an unprotected connection between two computers and detects important sequences of numbers (most often by the penetration of unprotected routers). After identifying addresses, computer accessed disconnect the lawful user, and the threat agent take control over access to files.
• *Masquerading* – usually is associated with registration of information and playing their further investigation. Is the type of attack in which an entity claim that is a different entity that have consisted the threat is usually one in which the threat agent displaces or modify messages or information;
• *Degradation of service* – takes place when an entity can`t fulfill their functions from the normal technical parameters.
• *Denial-of-service* – takes place when an entity can`t fulfill their functions, i.e. when a threat agent do actions that prevent an entity to fulfill their functions. Denial-of Service attacks (DoS) consist in a flooding IP addresses with data, and consequently, blocking his and their Internet. Most DOS attacks are launched against the servers, or websites, in order to prevent their visits by ordinary users. At the same time, may be launched and attacks more powerful - distributed DoS type (DDoS).
• *Software piracy* - is the type of threat that consists in "breaking" shareware programs, or that require a specific code serial.
• *Unauthorized copying date* – takes place after the threat has managed to penetrate the security system of the target computer and has access to the information on it;
• *Logical bombs* – are small programs or procedures that are inserted into an application and can be activated by a predefined event
• *Viruses* - according to RFC 1135 (The Helminthiasis of the Internet) "a virus is a sequence of code that is auto-inserting into a host of including in the operating system, in order to propagate. It cannot run independently. It requires the execution of the hosted program to activate". Therefore, viruses are malicious informatics programs, placed in the computer memory, which at one time can become active, affecting by destruction or deterioration, or by self coping in the files located on different magnetic devices. Each program infected may, at his turn, infect other programs.
• *Worms* - Worms are self-contained programs, able to multiply, to be transferred to other computers and, possibly, to carry out operations of massively. According to RFC 1135 "a worm is a program that can run independently, which consume the resources of the host to run and that can propagate a functional version of it to other computers". They work by the principle of "search and destroy".
• *Trojan horses* - is an application that seems to run a function very known and which, in a hidden, fulfills another function.
• *Trap doors* – trap doors are programs that create a "gate" (a new user) to allow access to the computer in question, or to grant special privileges for a particular user.
• *Excess privileges* - involves the granting of undue privileges, by administrative methods, or by unidentified penetration of the list for granting privileges to persons who have the right for such privileges.
• *Data diddling* - takes place after the threat agent has managed to penetrate the security system of the target computer, has access to the information on it, which destroy them.

5. Information Security Management Systems

Data protection is not a simple process that can be summarized in a password based access to users who have the right of access to information, such as the use of an information security management system became a requirement for organizations because on the states began adopting mandatory data protection legislation and information, but also because of attacks on organizations that may have severe negative consequences such as stealing and selling confidential strategies by competitors, branch and technological secrets, theft and using for illegal purposes of customer data etc.[5].

To ensure security, safety rules should be developed implemented through special techniques. Developing these rules, the following requirements must be considered: security requirements for the computer

[5] Susanto, H. & Almunawar, M. N. & Tuan, Y. C. (2011). "Information Security Management System Standards: A Comparative Study of the Big Five", *International Journal of Electrical & Computer Sciences IJECS-IJENS* Vol:11 Nr: 05, p. 23, October.

system and computer networks (physical and logical components and assembly information stored and transferred) and the specific requirements of the organization, on keeping confidentiality of certain data and hierarchy of access rights to information. In this regard, the development of a system of information security to consider two aspects: internal aspect protection programs, hardware and data and external appearance on the rules of protection set. Complexity of security problems is both technical and subjective, since the implementation of a security system requires its use by different categories of users. In this regard, efforts of specialists should be directed on several levels: strategic for developing security policies, technical realization and pragmatic protection mechanism for implementing the security system.

The security of a system is to define and implement security policies, standards and best practices and techniques used to prevent external attacks, unauthorized use of resources, and resource availability for authorized users and ensure system recovery in case of incidents or disasters. Securing information system is crucial in the development work of an organization as a result have developed special procedures for both security strategy development and its implementation. For this purpose are used in security systems standards.

International Standard ISO/IEC 27001 are a referential for evaluating security techniques implemented information security management systems.

This standard was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) and applies to all types of organizations (e.g. companies, agencies governmental, non-profit organizations).

The standard specifies requirements for the implementation of security measures tailored to the individual needs of the organization or parts thereof, so that information security management system to ensure proper selection of safeguards to protect computing resources and maintain the confidence of the parties involved.

ISO (International Standardization Organization) and IEC (International Electrotechnical Commission) are specialized international standardization system. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization specific fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Participate in this action and other international organizations, governmental and non-governmental. Information technology, ISO and IEC have established a joint technical committee ISO/IEC JTC 1. International Standards ISO/ IEC 27000 series were developed by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security Techniques.

ISACA - ITGI has secured ISO 27000 series of standards convergence, by mapping the standard over COBIT processes. By switching to the new architecture COBIT 5 ITGI proposed new framework will also ensure compliance with these security standards.

International Standard ISO/IEC 27001 provides a model for implementing the principles governing risk assessment, security planning and implementation, security management and review.

Adoption ISMS should be a strategic decision for an organization. Designing and implementing an ISMS in an organization is influenced by the needs and objectives, security requirements, the existing processes and the size and structure.

6. Conclusions

As the organizations and, by default, the critical infrastructures are becoming increasingly dependent on the proper functioning of information systems; the issue of security of these systems is becoming increasingly important.

Since the information society becomes more and more important both for financial accounting, business and for society, ensuring the security both for infrastructure, and for information that circulates on it, represents a critical point. Because the Internet is an environment of trust of information society, it must become available; the information transmitted or stored to be kept undisclosed and is necessary to be ensured the integrity, authenticity and non-repudiation of information.

Bibliography

[1] Șerb A. (2010). *Securitate informatică* – Editura Pro Universitaria, București.

[2] Șerb A., Baron C., Isăilă N., Ionescu C., Defta C. L. (2013). *Securitatea informatică în societatea informațională* – Editura Pro Universitaria, București.

[3] Interagency Working Group on Cyber Security and Information Assurance, S.U.A. (2006). *Federal Plan for Cyber Security and Information Assurance Research and Development*.

[4] Susanto, H. & Almunawar, M. N. & Tuan, Y. C. (2011). "Information Security Management System Standards: A Comparative Study of the Big Five", *International Journal of Electrical & Computer Sciences IJECS-IJENS,* 11(5), p. 23, October.