Risk Analysis of Accounting Information System Infrastructure

MIHALACHE, Arsenie-Samoil
"Alexandru Ioan Cuza" University - Iasi, Romania - Faculty of Economics and Business Administration - Doctoral School of Economics

01. February 2011

Risk Analysis of Accounting Information System Infrastructure

PhD Student MIHALACHE D. Arsenie-Samoil
"Alexandru Ioan Cuza" University - Iaşi, România
Faculty of Economics and Business Administration - Doctoral School of Economics
arsenie.mihalache@yahoo.com

Abstract: National economy and security are fully dependent on information technology and infrastructure. At the core of the information infrastructure society relies on, we have the Internet, a system designed initially as a scientists' forum for unclassified research. The use of communication networks and systems may lead to hazardous situations that generate undesirable effects such as communication systems breakdown, loss of data or taking the wrong decisions. The paper studies the risk analysis of the accounting information system in modern corporations from the viewpoint of modernising accounting against the background of implementing new information technologies aimed at carrying out the objectives of integration and globalisation construed as phenomena specific to information society and knowledge.

Keywords: attackers, threats, vulnerability, security, risk analysis.

JEL Classifications: M4, C8, D5, L1, L6, L8, P5

1. INTRODUCTION

The phenomena marking the economic environment over the last decades have been under the sign of globalisation, interdependence, and interaction. Whatever happens in any part of the world may have a minor or major impact on the local economic environment. Under these circumstances, any company regardless of its operations, size, and area of operation, has to prove its viability, capacity of communication, and adjustment with a view to achieving economic and financial performance that would make it increasingly competitive.

The development of the latest information and communication technology has led to building up company-integrated systems that make storage, access to, and transfer of information increasingly easier and more accessible. By implementing such systems, companies are enabled to build up flexible information infrastructures that are easily adaptable to changes in their operational environment, hence revolutionising their way of conducting operations (Andone et al. 2010).

Accounting is a formal language of business communication, which allows the company to be represented internally and externally. It should also be able to adjust quickly to the new global business environment undergoing continuous change and transformation. This adjustment would be impossible without the assistance of the new information technology and computer infrastructure revolving around the Internet. The use of communication networks and systems may be hazardous as it may encounter unexpected occurrences such as breakdown of communication systems, loss of information, or taking the wrong decisions.

If we consider a corporation from this perspective, the accounting system is regarded as the most important element of the corporate information system due to the following reasons (Andone and Tabara, 2006):

- the accounting information system is the only system that allows management and external users to have an overall picture of the company;
- the accounting information system connects other major information subsystems such as marketing, human resources, research and development, production, etc., to such an extent that all the information provided by these subsystems may be expressed ultimately in financial terms;
- the non-financial information in areas such as social responsibility and human resources are integrated with the accounting information to allow the decision-making process;
- the integration of accounting with the other subsystems leads to offering more accurate information to users at a higher speed.

The phrase information infrastructure refers to information resources, including communication systems, entities and people with expertise in the field. Examples of infrastructures are the corporate information infrastructure, the defence information infrastructure, the national information infrastructure as well as global information infrastructure (Aanestad et al. 2007).

2. ATTACKERS

The main sources of risk the accounting information systems may face are the people within a corporation and accidents or natural disasters. Moreover, people outside the company represent an important source of risk, in some cases, as they are more motivated and difficult to detect and investigate than the people inside the company.

The following 'agents' are likely to cause security-related problems to the accounting information system:

- Employees. They are invested with trust and they have access to the information system, which may enable them to develop a better knowledge of the system's weak points, they can conduct operations detrimental to the company, and they may delete digital records as well;
- Consultants / System servicing personnel. These people have frequent access to sensitive areas of the information system, which may enable them to conduct a wide range of operations;
- Suppliers / Customers. Their economic reasons are not always consistent with those of the customer / supplier and, sometimes, they may undertake actions that are likely to pose security-related risks;
- Competitors. Other individuals or companies likely to gain from losses incurred by the company resulting from such attacks on the information system;
- Crackers1/ IT mercenaries / Professional criminals. People that illegally penetrate information systems and intentionally cause damage, whose motivation is generally diverse;
- Espionage experts. They are professionals in obtaining information on behalf of other companies. These people have highly technical expertise; they are well trained and can most often pursue their interests without being detected;
- Accidents / Natural disasters can cause loss of important information or they can make them unavailable.

Attackers of information systems usually fall, according to their motivation, into four main categories such as:

- Social motivation. Attackers in this category try to gain a feeling of superiority or control, of acceptance of other attackers or of integration in a certain group.
- Technical motivation. Attackers in this category try to 'beat' the system, as a kind of intellectual challenge.

- Political motivation. Attackers in this category try to obtain political attention in order to promote a certain cause.
- Financial motivation. Attackers in this category try to gain personal benefit (i.e. spies, IT mercenaries, various companies, or even people that deal with confidential information, etc.).

Attacks on accounting information system infrastructure may have various forms. First, attacks can be classified according to the location where the attack is conducted. We can distinguish two kinds of attacks: on-site or remote. A second classification can be made according to the way the attacker interacts with the information following a successful attack. This leads to two categories of attacks, i.e. passive and active ones.

In most cases, one should be able to cope with the following types of attacks: computer viruses, Trojan horses and backdoors, password crackers, scanners, traffic sniffers, and social engineering attacks. Computer virus is a general term that describes various types of attacks on the infrastructure. As the existence of a malicious code in the computing systems may act differently due to the very design of the code, one should consider the various classes of malicious "programmes" – e.g. viruses, worms, Trojan horses, bombs, trapdoors / backdoors, spoofers, hoaxes, etc. – whenever one refers to such programmes.

A password cracker is a programme that may crack passwords, by-pass or deactivate password protection. Among the techniques used to "guess" the password, attack by "brutal force" and attack by use of dictionaries are commonly used.

The scanner is a utility application used to detect automatically the weak points in the security of a system. By means of a scanner, a user will be able to check, on-site or remotely, the entry points to penetrate a system and, later, to cover such security gaps. If an ill-intended person who masters the required knowledge uses such an instrument, the security of the information system infrastructure will be seriously affected. Initially designed to enhance it, scanners reaching the other side of the barricade may cause severe problems in ensuring security.

A sniffer is a software or hardware component, designed to "eavesdrop on" and "grab" the information transferred via the network. In order to sniff the traffic, certain conditions are required: the network architecture or the configuration of the network board should allow this to happen promiscuously. Placing a sniffer inside a network is possible only if either the attacker finds a gap in the security system or she or he is an employee of the corporation that wishes to collect classified information.

Social engineering attacks use human nature to secure access to classified information. Such attacks most often target credulous people among the organisation personnel.

Attacks on databases display some particular features as compared to the other information in the corporation, namely databases represent the largest amount of information the corporation operates with; databases can reveal personal details by processing public information. The main types of attacks on databases are direct, indirect, and by monitoring. Countermeasures can be applied to such attacks in order to block them or limit their effects such as antivirus software, firewalls, traffic analysers, patches, fixes, hotfixes, safe operating systems, safe applications, adequate passwords, and user's education.

3. THREATS

Threats affecting the infrastructure of the accounting information system represent actions, possible or taken, that might attack the system.

Threats directed against security fall into three categories: natural/physical, accidental, and deliberate. The deliberate ones are the most frequent. They fall into two categories: internal and external. Internal threats come from inside the corporation where its employees can easily access information, because there are fewer barriers they need to overcome. In addition, they are familiar with the corporate security policy. External threats come from many categories such as foreign intelligence agencies, terrorists and terrorist organisations, criminals, raiders, hackers and crackers.

Threats at the infrastructure of the accounting information system can be classified as follows: fundamental threats, facilitating threats, and indirect threats. Fundamental threats represent what an attacker wants to do. Such threats are information leaks, tampering with information, rejection, denial of service, and illegitimate use. Facilitating threats represent those threats that allow access to fundamental threats. Facilitating threats can be classified as masquerade, malicious programmes, security by-pass, and authorisation breech. Indirect threats derive from the basic characteristics of the Internet and of the information infrastructure, e.g. interception, scavenging, indiscretion and administrative error.

4. VULNERABILITY

Vulnerability can be defined as weakness in terms of system procedures, system architecture, system implementation, internal check, and other causes that may be exploited to penetrate security systems and to have unauthorised access to information (Bishop 1999). The main weak points of the infrastructure of the accounting information system are physical, natural, hardware, software, storing environment, radiations, communications, and human.

Universal vulnerability is defined as a state within an information system that:

- allows an attacker to execute commands as if she or he were an authorised user;
- allows an attacker to access information against the access protocols;
- allows an attacker to conduct a denial of service attack.

Exposure is the state of an information system that is not a universal vulnerability but which:

- allows an attacker to carry out activities to collect information about the system;
- allows an attacker to hide her or his illegitimate activities;
- includes a function that may be easily compromised;
- is a port of entry an attacker may use to access the system or the information therein;
- is construed as a problem from the point of view of the information system protocols.

5. SECURITY

Ensuring security of information involves carrying out four objectives: confidentiality, integrity, availability, and non-repudiation. Security is not an aim in itself. Security as an objective may be construed as a state. Security is never perfect, irrespective of the measures taken to this effect. There will always be an unthought-of gate via which the accounting information system may be attacked (Oprea 2007).

Security technologies designed to remove risks and limit loss are access control, firewall, antivirus software, file encryption, digital identification, physical security, etc. They are designed to limit access to information. Besides restricting technologies, infrastructure system security needs to be administered, monitored, and serviced. To this effect, the following operations have to be performed: prevention, detection, and response to intrusions.

Within information systems, encrypting is apparent on several layers, namely hardware, application, data transmission, files and folders.

Antivirus software is a utility that detects the action of a malicious programme and annihilates it. The antivirus software will detect the presence of a malicious code (virus) in the computer by using the signature left behind by such malicious programme (virus). Once the presence of a virus has been detected, the antivirus software will launch a subroutine, the vaccine that will annihilate the action of the virus. When selecting antivirus software, we should consider several criteria such as: workstation, the number of viruses it can detect, the time required to respond to a virus, network scanning options, e-mail scanning options, protection from scripts, compressed files scanning, presence of technical support, the length of time free updating is provided, the name of the software producer, location of the software company and of the dealer, and the price. Corporations or enterprises may face problems when using antivirus software. Virus scan, for example, is difficult to perform from each workstation, updating is difficult from each workstation, monitoring the performance of antivirus software on every workstation is difficult. Therefore, it is necessary to use an antivirus programme that would allow protection and monitoring from a single console, with safe and constant updating and centralised management.

A firewall is a system used to implement policies designed to control access to a corporate system or among corporations. It will protect a computer or a network from unauthorised access. In choosing a firewall, one needs to consider the following criteria: the degree of security, the operation system, and the administration one.

An intrusion detector is a process that detects and responds to abusive use of the accounting information infrastructure components. The use of an intrusion detector will create benefits for the company with respect to detecting, blocking, response to attacks, support in assessing damages incurred as well as evidence admissible in court against people charged with abusive use of infrastructure components. According to the specificity and the size of the company, one can opt for a certain type of intrusion detector. In small enterprises, such intrusion detectors are embedded in the firewall installed. Analysis of firewall logs or router will signal the intrusive attempts. Moreover, operating systems can facilitate detection of intrusions.

6. RISK ANALYSIS

Risk can be defined as a potential threat that may exploit weaknesses of the accounting information systems. Risk is an expected event. To prevent an event likely to affect the security of the information system from occurring, specific measures should be taken. Such measures are called security measures.

Risk analysis involves a process of identifying security risks, of determining the extent of such potential risks, and of identifying the high-risk areas that need to be secured. Risk analysis is part of a comprehensive body of measures called risk management. Risk assessment is a result of risk analysis. Risk management can be defined as the body of methods aiming at identifying, checking, removing or minimising events that may affect the resources of the system. This body includes risk analysis, cost analysis, selection of mechanisms, assessment of security measures implemented, as well as overall assessment of security.

Risk can be approached from many angles from among which some are presented below: quantitative analysis, qualitative analysis, and workstation analysis. These risk analyses are conducted mainly within large corporations and within some medium-sized enterprises. Small enterprises have neither specialised personnel nor the money to pay for such an assessment. Nevertheless, a minimum of security measures must be taken. It is a well-known fact that company managers are reluctant to invest in something that has no direct profit. When they are persuaded by the necessity of allocating the amounts required by ensuring security, such amounts are usually below the limit of the requirements. Under these circumstances, the entity needs to ensure such a security system whose expenses do not exceed the amount allocated. This can be labelled financially constrained security. There are two alternative solutions to this situation, i.e. covering threats that are most likely to occur, while preserving the initial checking methods or covering all threats and reducing costs as to checking measures.

The former allows for a maximum degree of protection against some threats, but may leave partially or completely uncovered threats. The latter requires reduced expenditure needed to ensure checks for a specific threat so that all possible threats may be covered. This can be reflected by modifying and configuring checking measures. This measure is to be preferred over the former as it does not allow for vulnerabilities to be uncovered by checking measures (Blakley et al. 2002).

Security is difficult to quantify but it can be appreciated as high, medium, low, or missing. Nevertheless, security level can be quantified at least form a financial point of view. Implementing or testing and upgrading a security system will always generate costs related to equipment and human resources.

Setting forth a security programme is the process via which the corporation or enterprise ensures its security. This programme involves five steps, namely appointing the personnel in charge with ensuring security, determining the main stages of implementing security, defining requirements of upgrading security, informing the personnel as to the required security measures, auditing, and monitoring security. There are cases where ensuring security involves hiring specialised organisations. They can conduct both the study and implementation, or only the study, while implementation is to be conducted with the company's own personnel. Specialised services are often hired by small-sized enterprises or when upgrading qualifications of the personnel in charge with ensuring security requires high costs. Outsourcing represents the company's option for security services ensured by a third party. If this is the case, we refer to a Security Service Management Supplier (SSMS). They provide both security services and the management thereof. Security Service Management (SSM) will be conducted not by the company but by the services supplier. Security is not a destination, it is an on-going process.

7. CONCLUSIONS

As corporations and enterprises become increasingly dependent on the reliable operation of the accounting information systems, the issue of system security becomes paramount. The infrastructure of the accounting information security in modern corporations relies on communication networks, which are generally open structures to which a large and varied number of components can be connected, hence a twofold potential vulnerability of the infrastructure can occur: tampering with information and unauthorised use thereof. In order to ensure the security of the accounting information system, the implementation of some specific mechanisms is of utmost importance. Such implementation start from the physical level (physical protection of transfer lines), the procedures blocking access to networks (firewall software), applying data encoding techniques (encryption), i.e. a specific method of protecting communication among applications running on various computers in the network. From among the causes of communication network vulnerability, we mention programming errors in the applications and their poor documentation, unsuitable configuration of the hardware and software elements, lack of support from the manufacturers, poor knowledge of or security issues or ignorance thereof.

The points presented in the paper enable us to consider the digitised environment as generator of new risks. In order to ensure efficient protection of data, it is necessary for any corporation to develop complex risk assessment and analysis.

The reality around us requires a three-fold approach of the risks the accounting information infrastructure faces, i.e. threats regarded as events or activities (generally from outside the system assessed), which may affect the vulnerabilities within any system, causing thus the impact, understood as a loss or a consequence the corporation or enterprise may suffer on a short, medium or long term. Risk within a corporation cannot be removed altogether, it will always be there. What corporation management can do is to reduce it to a manageable degree.

8. ACKNOWLEDGMENTS

This work was supported by the European Social Fund in Romania, under the responsibility of the Managing Authority for the Sectoral Operational Programme for Human Resources Development 2007-2013 [grant POSDRU/88/1.5/S/47646].

Referances

Aanestad, M., Monteiro, E., Nielsen. P., (2007). Information Infrastructures and Public Goods: Analytical and Practical Implications for Spatial Data Infrastructures. *Information Technology for Development*, 13(1), 07-25.

Adams, J., and Thompson, M., (2002). Taking account of societal concerns about risk: framing the problem, *Health and Safety Executive*, Research Report 035.

Amor, D., (2001). *The E-Business (R)evolution: Living and Working in an Interconnected World* (2nd Edition). Prentice Hall.

Andone, I., Dologite, D., Mockler, R., Tugui, A., (2001). *Dezvoltarea sistemelor inteligente în economie. Metodologie si studii de caz*, Ed. Economica, Bucuresti.

Andone, I., Pavaloaia, D., Bâcâin, I., Genete, L.D., (2004). *Modelarea cunoasterii în organizatii. Metodologie obiectuala pentru solutii inteligente*, Ed. Tehnopress, Iasi.

Andone, I., Pavaloaia, D., (2010). *Modelarea afacerii. Întreprindere-procese-reguli*, Ed. TIPO, Iasi.

Andone, I., Georgescu, I., Toma, C., (2010). *Cercetarea avansata in contabilitate*, Editura Wolters-Kluwer, Bucuresti.

Andone., I., Tabara, N., (2006). *Contabilitate, tehnologie si competitivitate*, Editura Academiei Române.

Andone, I., Vergara, M., Pavaloaia, D., (2010). *Modelarea afacerii. Întreprindere – procese – reguli*, Ed. TipoMoldova, 2010

Austin, R. and Darby, C., (2003). The myth of secure computing. *Harvard Business Review*, 81(6): 120-126.

Berryman, P. (2002). *Risk Assessment: The Basics*.

Bishop, M., (1999). Vulnerabilities Analysis. *In Proceedings of the Second RAID Conference*.

Blakley, B., McDermott, E. and Geer, D. (2002). Information security is information risk management. *In Proceedings of NSPW*, Cloudcroft, New Mexico, USA.

Bontchev, V.V., (1998). *Methodology of Computer Anti-Virus Research*, PhD thesis. University of Hamburg, Germany.

Buffam, W.J., (2000). *The Fundamentals of Internet Security*, Unisys.

Castano, S., Fugini, M., Martella, G. & Samarati, P. (1995). *Database Security*. Addison-Wesley.

Cohen, F., Phillips, C., Swiler, L.P., Gaylor, T., Leary, P., Rupley, F., Isler, R. and Dart, E. (1998). *A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses: A Cause and Effect Model and Some Analysis Based on That Model*, Sandia National Laboratories.

D'Arcy, S.P., (2001). Enterprise Risk Management. *Journal of Risk Management of Korea*, 12 (1).

Frisch, Æ., (1995). *Essential System Administration*, Second Edition. O'Reilly & Associates, Inc., CA, USA.

Jacobson R.V. (1996). CORA Cost-of-Risk Analysis. *In Proceedings of IFIP'96 WG11.2. Samos*, Greece.

Kabay, M. E. (1996). *Enterprise Security: Protecting Information Assets*. McGraw-Hill.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y., Wei, K.K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management* 23: 139-154.

Landwehr, C.E., (2001). Computer security. *International Journal of Information Security*, 1: 3 –13.

Loscocco, P.A., Smalley, S.D., Muckelbauer, P.A., Taylor, R.C., Turner, S.J. & Farrell, J.F. (1998). The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environment. *In Proceedings of the 21st National Information Systems Security Conference*.

Neumann, P.G. (1995). *Computer related risks*. ACM Press.

Oprea, D., (2007) *Protecţia şi securitatea informaţiilor*, Editura Polirom, Iasi.

Ozier, W., (1999). *A Framework for an Automated Risk Assessment Tool*, The Institute of Internal Auditors.

Panko, R.R., (2004). *Corporate computer and network security*. New Jersey: Prentice Hall.

Pfleeger, C.P., (1997). *Security in Computing*. Addison Wesley.

Schneier, B., (2000). *Secrets and Lies: Digital Security in a Networked Worl*d. Wiley: New York.

Siponen, M.T., (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8/1: 31-41.

Stallman, R.M., (1984). Letter to ACM Forum. *Communication of the ACM*, 27 (1), January: 8-9.

Stoneburner, G., Goguen, A., and Feringa, A., (2001). *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology.

Straub, D.W., şi Welke, R.J., (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22, 4 : 441-64.

Summers, R.C., (1997). *Secure Computing: Threats and Safeguards*. McGraw-Hill.

Vasiu, L., and Vasiu, I., (2004). Dissecting Computer Fraud: From Definitional Issues to a Taxonomy. *In Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii, USA. IEEE Computer.

Vasiu, L., and Vasiu, I., (2004a). A Taxonomy of Malware Use in the Perpetration of Computer-related Fraud. In U.E. Gattiker (Ed.), *EICAR 2004 Conference CD-rom: Best Paper Proceedings*. Copenhagen: EICAR e.V.

Vasiu, I., and Vasiu, L., (2001). *Totul despre hackeri*. Editura Nemira: Bucureşti.

Wilsher, R.G., şi Kurth, H., (1996). Security assurance in information systems. In Sokratis K. Katsikas şi Dimitris Gritzalis (Eds.) (1996). *Information Systems Security: Facing the information society of the 21st century*. Chapman & Hall.