Audit for Information Systems Security

Ana-Maria SUDUC[1], Mihai BÎZOI[1], Florin Gheorghe FILIP[2]
[1]Valahia University of Targoviste, Targoviste, Romania,
[2]Romanian Academy-INCE &BAR , Bucharest, Romania,
suduc@ssai.valahia.ro, bizoi@ssai.valahia.ro, ffilip@acad.ro

The information and communication technologies advances made available enormous and vast amounts of information. This availability generates also significant risks to computer systems, information and to the critical operations and infrastructures they support. In spite of significant advances in the information security area many information systems are still vulnerable to inside or outside attacks. The existence of an internal audit for information system security increases the probability of adopting adequate security measures and preventing these attacks or lowering the negative consequences. The paper presents an exploratory study on informatics audit for information systems security.
***Keywords**: Information System Risks, Audit, Security*

1 Introduction

The digital world phenomenon, on the one hand, offers tremendous benefits, but on the other, it also creates significant and unprecedented risks. Web technology allows users quick and inexpensive access to a large amount of information provided on websites, digital libraries or other sources of data [1]. The same factors that generate the benefits – speed and accessibility – if not properly controlled can leave the information systems (IS) vulnerable to fraud, sabotage, and malicious or mischievous acts [2]. There are many and varied security techniques which can be applied. The selection of one or a set of security techniques must be done according to the potential risks. Therefore, the first step to provide security is to identify the risks. Afterwards there must be selected those techniques (usually only one security measure is not enough) which together will provide the appropriate level of security for the data, for the systems and for the organization. A risk-based audit program will improve the organization security system.

2 Security risks

There are two categories of risks against which an information system must be protected: physical risks and logical risks. The *physical risks*, which are related more with the equipment than with the information system itself, includes natural disasters such as earthquakes, hurricanes, tornadoes and floods, as well as other dangers such as bombings, fires, power surges, theft, vandalism and unauthorized tampering. Champlain [3] identified a list of controls that protect the information systems against these physical threats. These controls are: various types of locks, insurance coverage over hardware and the costs to recreate data, procedures to perform daily backups of the information system and data, off-site storage and rotation of the backup media to a secure location, and current and tested disaster recovery programs. The *logical risks* refers to unauthorized access and accidental or intentional destruction or alteration of the information system and data. These threats can be mitigated through logical security controls which restrict de access capabilities of users of the system and prevent unauthorized users from accessing the system.
All these measures are even more important in case of critical information systems.
According to Symantec [4], organizations today must address four main types of IT risks: security risks, availability risks, performance risks and compliance risks. The security risks represent the unauthorized access to information: data leakage, data privacy, fraud, and endpoint security. The security risks include also broad external threats, such as viruses, as well as more targeted attacks upon specific applications, specific users, and specific information. An Ernst and Young survey showed that security incidents can cost companies between 17 and 28 millions of dollars for each occurrence ([5] quoted by [6]). Another survey made during 13 years [7] with the help of 522 computer security practitioners in U.S. showed that virus incidents occurred most frequently (at 49% of the respondents' organizations). The second-most frequently occurred incidents were insider abuse of networks (44%) followed by theft of laptops and other mobile devices (42%). Figure 1 presents the key type of in-

cidents. Other authors [8] [6] [9] also observed that, even the companies security measures are focused on outside threats, a great percent of the risks, which sometimes exceeds 50% from the total number of risks, are originating from legitimate network users.

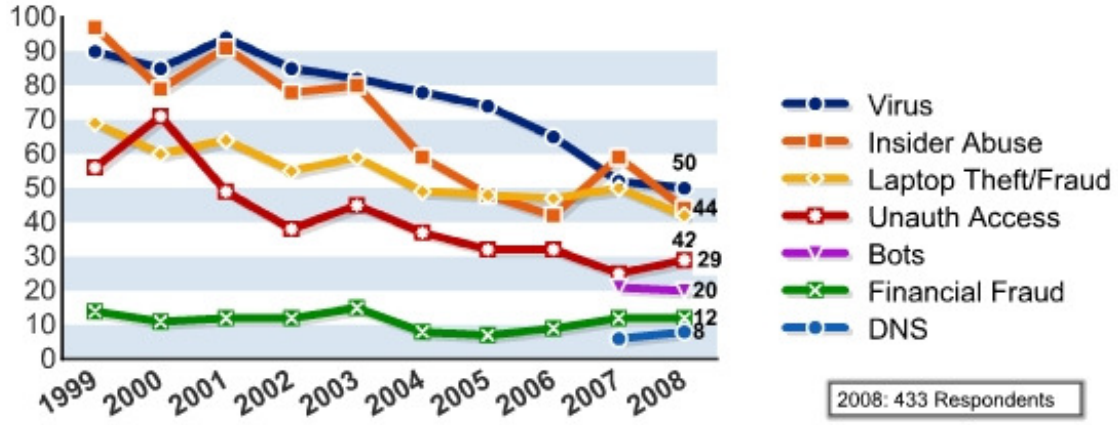

Fig. 1. Key type of incidents [7]

In 2008, a study made in Romania at Valahia University of Targoviste [1], on 126 technical engineering students, showed a high intentionality of information system misuse (46%). Regarding the motivation for IS misuse (Fig. 2), 41% motivated *curiosity*, 31% *personal gain without the intention to hurt someone*, 25% *intellectual challenge*, 3% answered *personal gain being aware of the negative consequences on others or on company*, and none of the engineering students answer that they would *intentionally harm others or the company.*

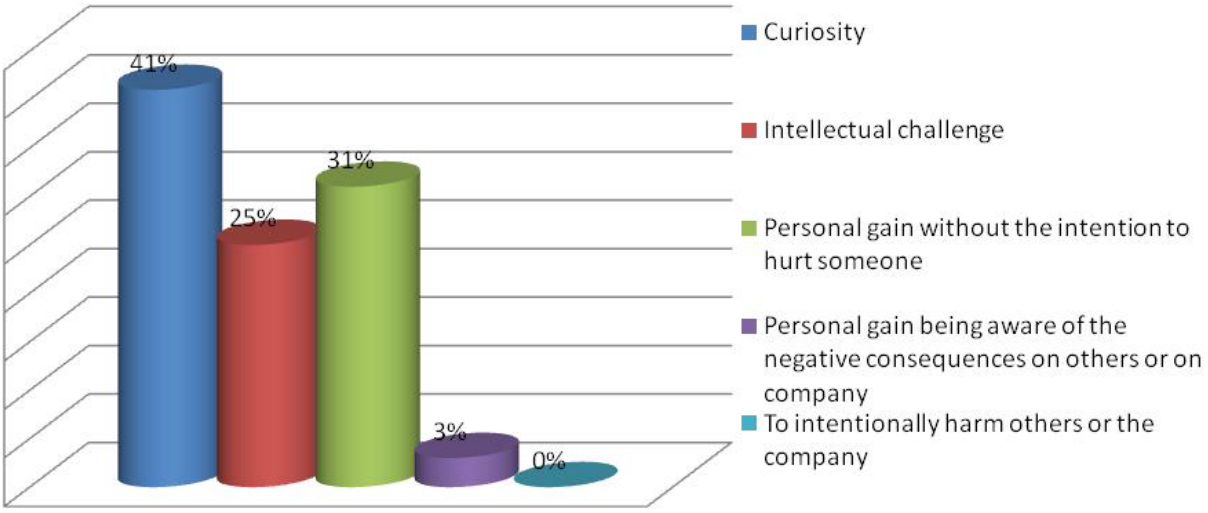

Fig. 2. Motivation for IS misuse

These results show that the security practitioners must give a significant attention to the measures which mitigate the insider threats.

Another interesting observation of this study was that most of the IS users are not aware of the ICT related risks or the IS security measures. For example to the question regarding to which extent they consider as a risk (from 1 to 5) the inside of the company attacks and the outside attacks, the respondents gave only 37% grades of 4 and 5 to the inside attacks and 31% to the outside attacks.

3 Audit for IS Security

Lampson [10] noticed that, in spite of significant advances in the information security area, such as subject/object access matrix model, access control lists, multilevel security using information flow and the star-property, public key cryptography, and cryptographic protocol, the many information systems are vulnerable to inside or outside attacks. Security setup takes time, and it contributes nothing to useful output and, therefore, if the setup is too permissive no one will notice unless there's an audit or an attack. This observa-

tion highlights the necessity of an internal audit for information system security in each organization.

Mukaila Apata, System Auditor and Security Administrator with over 18 years of experience consider [11] that three areas of the computer activity should be monitored on a regular basis: user access control, system activity monitoring, and the audit trail. These activities are closed to the basic mechanisms for implementing security proposed by [10]: (a) *authenticating* principals ("Who said that?" or "Who is getting that information?" - people, groups, machines, or programs); (b) *authorizing* access ("Who is trusted to do which operations on this object?") and (c) *auditing* the decisions of the guard ("what happened and why").

The aim of security in the *user access control* area is to optimize productive computer time, mitigate de risk of error and fraud, eliminate unauthorized access and secure the confidentiality of information. It is also obvious the necessity to permanently *monitor the system activity* because the malicious acts of sabotage or fraud are more likely to occur, if there are low chances of detection.

Apata indicated four questions which must be asked on probable areas of risk: (1) Could this happen here? (2) How? (3) Are security measures adequate to prevent/detect the threat? (4) How can we improve on the measures? [11]. The utilization of effective system security and controls can reduce considerable the incident occurrence and/or negative consequences by increasing the possibility of prevention and detection.

Another important security action is to maintain *detailed logs* of who did and when and also if there are any attempted security violations. All these information are very important for the system auditor.

3.1 Audit standards

According to ISO/IEC 18028-3, IT network security - Part 3: Security communications between networks using security gateways, audit is a "formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity". Audit [12] is a "formal inspection and verification to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. An Audit may be carried out by internal or external groups."

ISO reserved a series of standards, ISO 27000, for information security matters [13]:

- ISO 27001, published in October 2005, was created to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System";
- ISO 27002, the rename of the ISO 17799 standard, is a code of practice for information security which "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization";
- ISO 27003 is still in the proposal phase and aims to provide help and guidance in implementing an Information Security Management System;
- ISO 27004 was published in December 2009, and provides guidance on the development and use of measures and measurement for the assessment of the effectiveness of an implemented information security management system and controls, as specified in ISO 27001;
- ISO 27005 provides guidelines for information security risk management (ISRM) in an organization, specifically supporting the requirements of an information security management system defined by ISO 27001;
- ISO 27006, with the formal title formal "Information technology - Security techniques. Requirements for bodies providing audit and certification of information security management systems", is intended to be used in conjunction with a number of others standards and offers guidelines for the accreditation of organizations which offer certification and registration with respect to an Information Security Management System. This standard documents the requirements additional to those specified within standard ISO 17021, which identified the more generic requirements.

The most known and mature of these series of standards are the first two: ISO 27001 and ISO 27002. There are also other closely related standards, such as ISO 17021, BS7799-3, ISO 24760, ISO 13335 and BS25999.

The ISO 27003 focus on eleven control clauses: (1) security policy; (2) organization of information security; (3) asset management; (4) human resources security; (5) physical security; (6) communications and ops management; (7) access control; (8) information systems acquisition, development, maintenance; (9) information security incident management; (10) business continuity and (11) compliance.

Calder [14] observed that policy is owned by top

management and the other control clauses are operational responsibilities and he represented the relationship between the control clauses (Fig. 3).

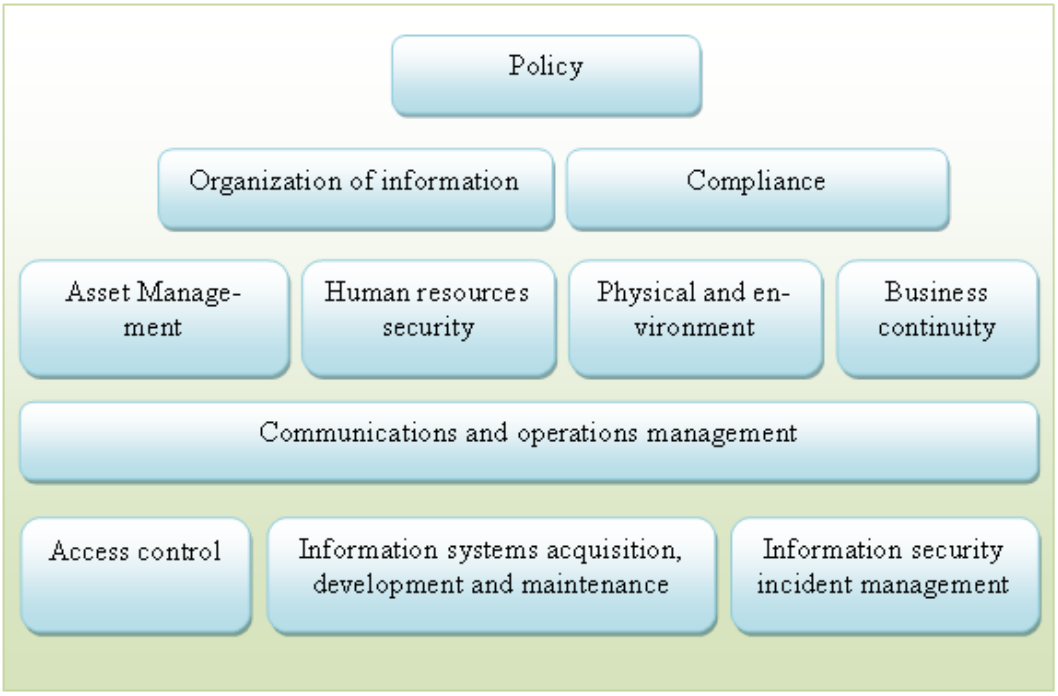

Fig. 3. Relationship between the control clauses

3.2 Audit plan

A security audit has the main objectives [15] to:

- Check the existence security policy, standards, guidelines and procedures;
- Identify the inadequacies and examine the effectiveness of the existing policy, standards, guidelines and procedures;
- Identify and understand the existing vulnerabilities and risks;
- Review existing security controls on operational, administrative and managerial issues, and ensure compliance to minimum security standards;
- Provide recommendations and corrective actions for improvements.

In order to ensure compliance of security policy and to determine the minimum set of controls required to reduce the risks to an acceptable level, the security audits should be conducted periodically (vulnerabilities and threats change with time and environment) [15]. The audits can be new installation / enhancement audits, regular audits, random audits or non-office hour audits.

The techniques used to the auditing process can include automated auditing tools (ready-made security audit systems and/or security auditors' own developed tools) or there can be manual review techniques (e.g. social engineering attacks and auditing checklists).

An audit process may include several steps. 3D Networks [16] proposed an audit process in seven steps (figure 4): (1) vulnerability scanning - scanning the infrastructure, (2) report audit - auditing reports like logs, intrusion detection systems reports, etc., (3) security architecture audit - auditing the existing security architecture, (4) baseline auditing - auditing the security setup to verify that it is in accordance with the security baseline of the organization, (5) internal control and workflow audit - auditing the existing workflow, (6) policy audit - auditing the security policy to ensure that it is in line with the business objective and (7) threat/risk assessment – assessment of the various risks and threats facing the company's information systems.

During and at the end of the auditing process a series of reports may be elaborated: a report with the vulnerabilities identified in the organization information system, a report with the threats and risks the organization faces as a result of the existing vulnerabilities including faulty policy, architecture, etc., and an audit report which gives the security overview and the results of all the audits.

Another perspective on the security audit process is provided by [15] which divides the audit in six steps: (1) planning - to determine and select effective and efficient methods for performing the audit and obtaining all necessary information; (2) collecting audit data - to determine how much

and what type of information to be captured, and how to filter, store, access and review the audit data and logs; (3) performing audit tests - general review on the existing security policies or standards/security configurations/Technical investigation; (4) reporting for audit results – present the current security environment; (5) protecting audit data & tools - safeguard the audit data and tools for the next audit or future use; (6) making enhancements and follow-up - make corrective actions if required.

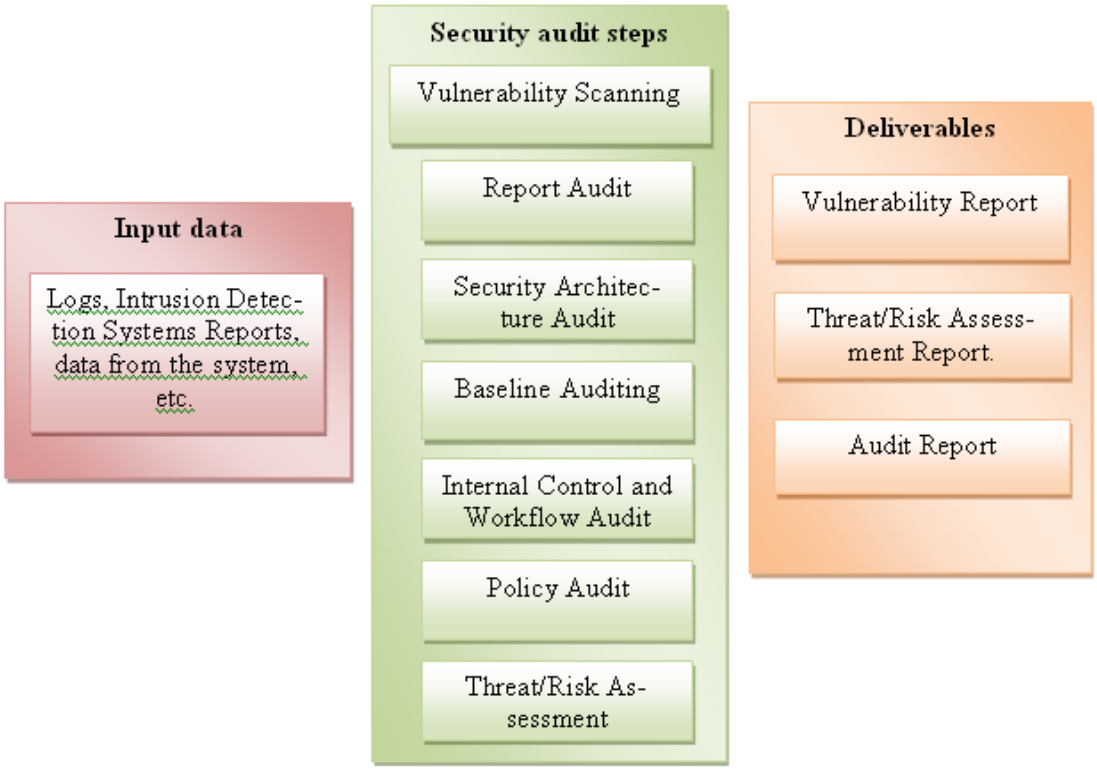

Fig. 4. Audit process

The security audit process is becoming more difficult to undertake with the growing complexity of information systems. There are automated auditing tools which significantly facilitates this process.

4 Conclusions

There are many and varied security techniques which can be applied. The selection of a set of security techniques must be done according to the potential risks. But in order to provide properly and effective protection to the organization assets, the security system (measures) must be assessed. Internal or external, a security audit is one of the best ways to determine the security efficiency.

There are a number of security audit standards which specify procedures that should be followed to ensure that IT resources are adequately safeguarded.

With still high losses due to inadequate IS security, a security audit must be considered by any organization.

References

[1] A. M. Suduc, M. Bizoi and F. G. Filip, "Ethical Aspects on Software Piracy and Information and Communication Technologies Misuse," *Preprints of IFAC SWIIS Conference*, Bucharest, 2009.

[2] NSAA and GAO. (2001, December). *Management Planning Guide for Information Systems Security Auditing.* Retrieved January 2010, from U. S. Government Accountability Office, Available at: http://www.gao.gov/special.pubs/mgmtpln.pdf

[3] J. J. Champlain, *Auditing information systems, second ed.*, Hoboken, New Jersey: John Wiley & Sons, 2003.

[4] A. M. Suduc and F. G. Filip, "Riscuri ale utilizarii inadecvate a sistemelor informatice (Risks of Information Systems Misuse)," *Studii si cercetari economice*, No. 72, 2008.

[5] A. Garg, J. Curtis and H. Halper, "Quantifying the Financial Impact of IT Security Breaches," *Information Management & Computer Security*, Vol. 11,

No. 2, 2004, pp. 74-83.
[6] P. Z. Manrique de Lara and D. V. Tacoronte, "Supervising Employee Misuse of Information Systems in the Workplace: An Organizational Behavior Study," *Empresa global y mercados locales: XXI Congreso Anual AEDEM. 1*, Madrid: Universidad Rey Juan Carlos, 2007, pp. 31-43.
[7] R. Richardson, *CSI Computer Crime & Security Survey*, 2008, Retrieved January 2010, from Department of Computer Science and Engineering, Available at: http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf
[8] J. D'Arcy, *Improving Information Systems Security through Procedural and Technical Countermeasures*, 2005, Retrieved June 23, 2009, from Irwin L. Gross eBusiness Institute, Temple University, Available at: http://ibit.temple.edu/research/ResearchReports/ISSecurityMeasures.pdf
[9] V. Gawde, *Information Systems Misuse - Threats & Countermeasures*, 2004, Retrieved January 2010, from InfosecWriters, Available at: http://infosecwriters.com/text_resources/pdf/information_systems_misuse.pdf
[10] B. W. Lampson, "Computer Security in the Real World," *Proceedings of the Annual Computer Security Applications Conference*, 2000.
[11] M. Apata, *The Essence of Information System Security and Audit.* Retrieved January 2010, from Jidaw.com, Available at: http://www.jidaw.com/security1.html
[12] *ITIL V3. Service Design*, Office of Government Commerce (OGC), 2007.
[13] ISO, *The ISO 27000 Directory*, 2009, Retrieved 2010, from http://www.27000.org/
[14] A. Calder, *Information Security Based on ISO 27001/ISO 27002 - A Management Guide (2nd ed.)*, Zaltbommel: Van Haren Publishing, 2009.
[15] OGCIO, *Security Risk Assessment and Audit Guidelines*, 2006, Retrieved January 2010, from Office of the Government Chief Information Officer, Available at: http://www.ogcio.gov.hk/eng/prodev/download/g51_pub.pdf
[16] Networks, 3. (n.d.), *Security Audit.* Retrieved 2010 February, from Scribd, Available at: http://www.scribd.com/doc/12734608/Security-Network-Audit-Steps

Ana-Maria SUDUC is currently assistant at the Automatic Control, Informatics and Electrical Engineering Department, Electrical Engineering Faculty, Valahia University of Targoviste, Romania. She has been involved in different ICT projects (research and educational) at national and international level. Her current research interests include interfaces for decision support systems, group decision support systems, and web interfaces.

Mihai BÎZOI is currently assistant at the Automatic Control, Informatics and Electrical Engineering Department, Electrical Engineering Faculty, Valahia University of Targoviste, Romania. He was/is involved in different ICT projects (research and educational) at national and international level. His current research interests include communications-driven decision support systems, group decision support systems, and web collaborative technologies.

Florin Gheorghe FILIP took his MSc and PhD in control engineering from the TU "Politehnica" of Bucharest. In 1991 He was elected as a member of the Romanian Academy (RA). He has been a scientific researcher at the National R&D Institute in Informatics (ICI) of Bucharest. Currently he is a part-time researcher at the National Institute of Economic Researches (INCE) of the RA, also the director of the Library of the Academy. He was elected as vice-president of RA in 2000 and re-elected in 2002 and 2006. His main scientific interests include large–scale systems, decision support systems, technology management and foresight.