Conducting an information security audit

~ Prof. Ph.D. Gheorghe Popescu (Academy of Economic Studies)
~ Prof. Ph.D. Adriana Popescu (Academy of Economic Studies)
~ University Junior Assistant, PhD Attendant Cristina Raluca Popescu (University of Bucharest)

Abstract: *The rapid and dramatic advances in information technology (IT) in recent years have without question generated tremendous benefits. At the same time, information technology has created significant, unprecedented risks to government and to entities operations. So, computer security has become much more important as all levels of government and entities utilize information systems security measures to avoid data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive information. Obviously, uses of computer security become essential in minimizing the risk of malicious attacks from individuals and groups, considering that there are many current computer systems with only limited security precautions in place.*

As we already know financial audits are the most common examinations that a business manager encounters. This is a familiar area for most executives: they know that financial auditors are going to exam - ine the financial records and how those records are used. They may even be familiar with physical security audits. However, they are unlikely to be acquainted with information security audits; that is an audit of how the confidentiality, availability and integrity of an organization's information are assured. Any way, if not, they should be, especially that an information security audit is one of the best ways to determine the security of an organization's information without incurring the cost and other associated damages of a security incident.

Key words: *Computer security audit, IT security, informational systems' audit, information security management system, IS security policies, firewall.*

Adapting to the New World

Management of information, one of the most valuable assets, critical to success, often requires guidance in what to do. While there are many information security models, none is universally accepted.

Management must provide the specific actions, policies, procedures, and controls. While each organization does it differently, those responsible include IS management, line management, the CISO (chief information security officer, assuming there is one), and the internal auditors.

High security threats are now normal rather than exception. In 2006 and part of 2007, over 67% of the infections classified by the Forum of Incident Response and Secu - rity Teams' (FIRST) Common Vulnerability Scoring System (CVSS), were high severity threats. The CVSS system, (a relatively complex and thorough model for characterizing the fundamental characteristics of a threat and measuring its impact), has no single definition for the vulnerabilities that would cause a high severity threat. As a general rule however, a high severity threat is one that allows an attacker to remove confidential data, take over, or otherwise modify a remote machine without authentication. Such a breach effectively leaves an organization at the mercy of an attacker, and can have negative consequences for a company.

Today, computer security comprises mainly "preventive" measures, like firewalls or an exit procedure.

A **firewall** can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and is normally implemented as software running on the machine, hooking into the network stack to provide real-time filtering and blocking. Another implementation is a so called **physical firewall** which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet. However, relatively few organizations maintain computer systems with ef - fective detection systems, and fewer still have organized response mechanisms in place.

An effective **exit procedure** consists of documented standard processes that are carried out for each person who has ceased employment as well as measures to ensure that cessations are detected and reported so the processes will be completed.

Does it Matter?

As we already know, yes it does, because the key to effective **information security** is to work smarter, not harder. And in this case, working smarter means investing our valuable time, money and human resources on addressing the specific problems that are the most likely to cause a lot of damage. *So we have first to identify the risks.* The answers of some questions will help us:

a) What are the resources, meaning the information systems? Are they enough important so we have to protect them?

b) What is the value of those resources, monetary or otherwise?

c) What are the all the possible threats that those resources face?

d) What is the likelihood of those threats being realized?

e) What would be the impact of those threats on our business or personal life, if they were realized?

If we answered these questions above,

we can then investigate both mechanisms technical and procedural, that might address those risks, and then weigh up the cost of each possible solution against the potential impact of the threat. So, the answer is simple: if the cost of the solution is higher then the potential financial impact of the risks being addressed is higher; then one may need to investigate other solutions, consider accepting and living with a part of the risk, or accepting and living with the risk completely.

A Computer Security Audit

A computer security audit is a systematic, measurable technical assessment of how the organization's security policy is employed at a specific time. According to this, **computer security auditors** work with the full knowledge of the organization, at times with considerable inside information, in order to understand the resources to be audited.

Security audits are part of the on-going process of defining and maintaining effective security policies, which involves everyone who uses any computer resources throughout the organization. Given the dynamic nature of computer configurations and information storage, some managers may wonder if there is truly any way to check the security ledgers. Security audits provide such a tool, a fair and measurable way to examine *how secure is an information environment.*

Computer security auditors perform their work through personal interviews, vulnerability scans, examination of operating system settings, analyses of network shares, and historical data.

Because a policy is typically published, and because it represents executive decision, it may be just what is needed to convince that potential client, merger partner or investor is really exactly who he pretend to be.

Increasingly companies are requesting proof of sufficient levels of security from the parties they link to do business with. They are concerned primarily with how security policies are actually used, that's way a security policy is exactly the place to start.

The complexity of a computer system cannot guarantee that it is free of defects. From some knowledgeable observers to ignore computer security efforts, the external threats, and generally treat the computer system itself as a trusted system, represent an enormous mistake. They also point out that, this ignorance is the cause of many cases of insecurities of current computer systems: once an attacker has subverted one part of a system without fine-grained security, this one usually has access to most or all of the features of that system. This kind of security attitude tends to produce insecure systems.

There are a number of **key questions** that security audits should attempt to answer:

- Are theirs passwords difficult to crack?
- Are there access control lists in place on network devices to control who has access to shared data?
- Are there audit logs to record who accesses data?
- Are the audit logs reviewed?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?

- Are these operating systems and commercial applications patched to current levels?
- How is backup media stored? Who has access to it? Is it up-to-date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind?
- How have these custom applications been tested for security flaws?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?

These are just a few of many questions that can and should be assessed in a security audit. In answering these questions honestly and rigorously, an organization can realisti - cally assess *how secure its vital information is.*

Defining the Security Policy

As stated, a **security audit** is essentially an assessment of how effectively the organization's security policy is being implement - ed. Of course, this assumes that the organization has a security policy in place which, unfortunately, is not always the case. Despite all of this it is possible to find organizations where a written security policy does not exist yet. Security policies suppose to standardize security practices by having them codified in writing and agreed to by employees who read them and sign off on them. If security practices are unwritten or they are just informal, they may not be generally understood and practiced by all employees in the organization. It is also necessary that all employees have read and signed off on the security policy; other way the compliance of the policy cannot be enforced. Written security policies are not about questioning the integrity and competency of employees; rather, they ensure that everyone at every level understands how to protect company data and agrees to fulfill their obligations in order to do so.

The security audit should seek to measure security policy compliance and recommend solutions to deficiencies in compliance. The policy should also be subject to scrutiny. Is it a living document, accurately reflecting how the organization protects IT assets on a daily basis? Does the policy reflect industry standards for the type of IT resources in use throughout the organization?

The Necessary Steps for the Pre-Audit Process

Even before the computer security auditors begin an organizational audit, there is a fair amount of "homework" that should be done. First of all auditors need to know what they're auditing; they must to review the re - sults of any previous audits that may have been conducted. They also need to find about the tools they will use or refer to before. All of these steps represent a technical description of the system's hosts. The auditors must find about the entity management. Several security questionnaires may be used as to follow up the entity survey. Maybe these questionnaires are apparently subjective measurements, but they are useful because they provide a framework of agreed-upon security

practices. The respondents are usually asked to rate the controls used to govern access to IT assets. These controls include: management controls, authentication/access controls, physical security, outsider access to systems, system administration controls and procedures, connections to external networks, remote access, incident response, and contingency planning.

Entity surveys and security questionnaires (Munteanu, 2001) should be clearly written by auditors with quantifiable responses of specific requirements. They should offer a numerical scale from least desired to most desired. Both should include electronic commerce considerations if appropriate to the client organization. For instance, credit card companies have compliance templates listing specific security considerations for their products. These measure network, operating system, and application security as well as physical security.

Auditors, especially the internal ones, should review previous security incidents at the client organization to gain an idea of historical weak points in the organization's security profile. It should also examine if current conditions are able to ensure that those incidents cannot occur. If auditors are asked to examine a system that allows Internet connections, they may also want to know about IDS/Firewall log trends. Do these logs show any trends in attempts to exploit weaknesses? Could there be an underlying reason (such as faulty firewall rules) that such attempts are taking place on an ongoing basis. How can this be tested?

Because of the breadth of data to be examined, auditors will want to work with the client to determine *the scope of the audit*, which must be clearly defined, understood and agreed to by the client. The audit process must include some others factors: the entity business plan, the type of data being protected and the value or the importance of those data for the client organization, the time available to complete the audit and the talent or the expertise of the auditors. It's also important to find about previous security incidents.

Next, the auditors will develop the *audit plan*, which must cover how will audit be executed, with which personnel, and using what tools. They will then discuss the plan with the requesting organization. Next they discuss the *objective of the audit* with personnel organization along with some of the logistical details, such as the time of the audit, which their staff may be involved and how the audit will affect daily operations. At this stage the auditors should ensure that audit objectives are understood.

The Auditing Process

Auditors use a set of specific audit techniques and procedures, such as (Dobroteanu & Dobroteanu, 2008): observation, interviews, questionnaires, collecting and studying internal regulations and relevant legislation, organizational charts, graphs, analyses and statistical comparisons, etc.

The evidences can be obtained by combining the techniques (Ali & Stanciu, 2004): direct observations, interviews, questioning, examination, and sampling.

At the beginning, the aim of the auditors is to conduct an entry briefing where they outline the scope of the audit and what they are going to accomplish.

The auditors should be thorough and

fair, applying consistent standards and procedures throughout the audit. During the auditing process, they will collect data about the physical security of computer assets and perform interviews of organization staff.
They may perform network vulnerability assessments, operating system and application security assessments, access controls assessment, and other evaluations. Throughout this process, the auditors should follow their checklists, but also keep eyes open for unexpected problems. They should look beyond any preconceived notions or expectations of what they should find and see what is actually there.

The ISACA "S14. Audit Evidence" audit standard recommends to the IS auditors to obtain sufficient and relevant evidences in order to ground as realistic as possible conclusions and to express relevant opinions.

These modern tools and techniques can assist the auditor in any phase of its mission, being used in order to (Nastase et al., 2007):

- Testing a system's security measures;
- Analyzing and controlling the informatics applications existent in the system;
- Identifying the risks for a an organization and assessing them;
- Evaluating internal control;
- Verifying files integrity;
- Analyzing the information of the audited client by complex interrogations of the data bases, extractions, layering, and totals.

After the audit is complete, the auditors will conduct an outgoing briefing, ensuring that management is aware of any problems that need immediate correction. Questions from management are answered in a general manner so as not to create a false impression of the audit's outcome. At this point in time it should be stressed that the auditors may not be in a position to provide definitive answers. Any final answers will be provided following the final analysis of the audit results.

The next step for auditors is to comb their checklists and analyze data discovered through vulnerability assessment tools. There should be an initial meeting to help focus the outcome of the audit results. During this meeting, the auditors can identify problem areas and their possible solutions. The audit report must be simple and direct, containing concrete findings with measurable ways to correct the discovered deficiencies.

The audit report can follow a general format of executive summary, detailed findings and supporting data, such as scan reports as report appendices. The report must include first the executive summary. It's important to realize that strengths as well as deficiencies can be addressed in the executive summary to help give an overall balance to the audit report. Next, the auditors can provide detailed report based on audit checklists. The audit findings should be organized in a simple and logical manner on one-page worksheets for each discovered problem. This worksheet outlines the problem, its implications, and how it can be corrected. Space should be left on the worksheet to allow the site to document corrective steps and a comment block to dispute the finding if appropriate.

The finally step for the audit staff is to prepare the report as speedily as accuracy allows so that the organization staff can correct the problems discovered during the audit. Depending on company policy, auditors should be ready to guide the audited organization staff in correcting deficiencies and

help them measure the success of these efforts. Management should continually supervise deficiencies that are turned up by the audit until they are completely corrected.

The Role of Audit of Information Security

While organizations evolve, their security structures will change as well and according to this, the computer security audit must be a continual effort to improve data protection. **Auditing Information Security** the auditors measures the organization's security policy and provides an analysis of the effectiveness of that policy within the context of the organization's structure, objectives and activities. The auditors must help organizations to refine their policy and correct their deficiencies that are discovered through the audit process. Whereas tools are an important part of the audit process, the audit is less about the use of the latest and greatest vulnerability assessment tool, and more about the use of organized, consistent, accurate, data collection and analysis to produce findings that can be measurably corrected.

To be effective in ensuring accountability, auditors must be able to evaluate information systems security and offer recommendations for reducing security risks to an acceptable level. To do so, they must possess the appropriate resources and skills.

Using a computer (Popescu et al., 2005) modifies the way in which financial information is processed, stored and communicated and it can affect both the accountancy system and the internal control system used by the entity. Consequently, a CIS (computerized information system) environment implies most times: large transactions volume – which makes is difficult to identify and correct errors during processing; automatic generation to another application of significant transactions or incomes; making complex calculation; automatic electronic exchange with other organizations, without revising values or their reasonability.

REFERENCES:

1. **Ali, E. & Stanciu V**. (2004), *Auditul sistemelor informatice (Information Systems Audit),* Bucuresti: Editura DuAl Tech
2. **Dobroteanu, C.L. & Dobroteanu, L.** (2008), *Audit intern (Internal Audit),* Bucuresti: Editura InfoMega
3. **Munteanu, A.** (2001), *Auditul sistemelor informationale contabile (Accountancy Information Systems' Audit)* Iasi: Editura Polirom
4. **Nastase, P. & Stanciu, V. & Ali, E. & Nastase, F. & Popescu, Gh. & Gheorghe, M. & Babeanu, D. & Boldeanu, D. & Gavrila,** A. (2007), *Auditul si controlul sistemelor informationale (Informational Systems Audit and Control),* Bucuresti: Editura Economica
5. **Popescu, Gh. & Popescu, V. & Popescu, C.** (2005) *Rolul auditorului de sisteme informationale in achizitionarea programelor informatice utilizate in activitatea financiara si contabila (The role of the information systems auditor in the acquisition of information software used in the financial and accountancy activity)* – Auditul Financiar, nr. 12: 16-20