Risks of cyber attacks on financial audit activity

Cristina Raluca POPESCU,
University of Bucharest, Bucharest, Romania,
E-mail: popescu_cr@yahoo.com

Gheorghe POPESCU,
Bucharest University of Economic Studies, Bucharest,
Romania, E-mail: Gheorghe.Popescu@cig.ase.ro

Abstract

Simultaneously with increasing the speed and precision of data processing, multiple connectivity, fast transmission over long distances, and their results, the development and generalization of automatic processing, brought many new vulnerabilities and deficiencies, otherwise inevitable, the basis of new risk categories. The risks of cyber attacks on financial auditing involve the risk management of information systems security. Identifying, mitigating or eliminating the effects are mandatory requirements without which a high-quality financial audit can not be achieved in a highly computerized environment. To substantiate specific risk management actions on information systems security, in this study we analyzed the main types and techniques used in cyber attacks by making their radiography, identifying the strengths and weaknesses of new technologies and systems that are or not favoring security systems. At the same time, we analyzed the security system of an information system, organized it in layers, and revealed the specific areas for the security evaluation of the Mehari method. Finally, some of the results of a survey based on a questionnaire made with the support of master students of the "Information Systems Audit and Control" course were revealed, with three of the most common weaknesses identified for each security domain.

Keywords: *risk, financial audit, IT security, risk management, cyber attack.*

JEL Classification: *D83, G32, K24, L86, M15, M41, M42*

To cite this article:
Popescu, C.R. and Popescu, G. (2018), Risks of cyber attacks on financial audit activity, *Audit Financiar*, vol. XVI, no. 1(149)/2018, pp. 140-147, DOI: 10.20869/AUDITF/2018/149/006

To link to this article:
http://dx.doi.org/10.20869/AUDITF/2018/149/006
Received: 27.06.2017
Revised: 12.09.2017
Accepted: 13.09.2017

Introduction

The technological evolution of the transmission, processing and storage of financial-accounting data has given rise to new concepts such as cloud computing, real-time accounting or mobile reporting but has also brought new threats to these new concepts. To hide intentions and evil deeds, criminals continue to refine their techniques and methods of computer attacks. Users are caught in the middle, becoming now, not only targets for attackers but also potential facilitators or even accomplices. Users have now become the most vulnerable link in the security system.

Literatura de specialitate relevă faptul că dezvoltarea tehnologică a dus la progresul extrem de rapid al amenințărilor la adresa securității informaționale. Deşi 2014 a fost definit la nivel global drept "anul atacurilor cibernetice", literatura evidențiază o tendință de creştere a numărului şi a impactului atacurilor cibernetice de la un an la altul, cu o dezvoltare acută a atacurilor asupra dispozitivelor mobile. Acest lucru demonstrează încă o dată faptul că problema securității informațiilor, gestionată prin intermediul noilor tehnologii, a devenit o prioritate maximă. Unfortunately, for reasons that are easy to understand, cyber attacks are not sufficiently popular. But when their effects can no longer be hidden, they are shocking by their magnitude. Examples in this sense are the big companies forced to discontinue their activities because their information system has become inoperable, or when the ATMs become inoperable for a period of time to create discontent or even panic. It is necessary to assess the impact of cyber attacks on multiple levels: legislative, technological, economic, social. Data security experts suggest that it is time to change security approach to achieve real security. More sophisticated controls must be implemented to help, providing preventative real protection, but also during and after an attack.

1. Cyber attacks, main types and techniques used

Current information systems are increasingly complex and include very heterogeneous equipment. These equipments are most often structured on a computer network. This is an open structure that can permanently connect new users and new types of equipment (terminals, laptops, workstations, servers, smart phones, personal computers, routers, various connectivity and retellation elements, etc.) virtually extends the circle of users with access to its resources (personal applications, distributed applications, various services, files, databases, shared hardware, various other shared resources). The vulnerability of the network is manifested on two distinct levels: the attack on the physical integrity of information (destruction or modification) and unauthorized use of information (leakage of information to unauthorized third parties to access that information). To counteract, eliminate or mitigate the effects of cyber attacks, these must be well known and analyzed. In the literature, cyber attacks are analyzed from several points of view. For the issue we approached, in accordance with (Tăbuşcă A., 2009) cyber attacks can be considered as passive attacks and active attacks. **Passive** attacks are all those attacks in which the intruder notices the information passing through the communication channel without interfering with the flow or content of the messages. It is basically only analyzing the intercepted traffic, discovering the identities of the communicating entities; the length and frequency of messages are revealed even if their content remains hidden. These attacks do not cause direct damage and do not violate confidentiality rules regarding their "spirit". The purpose of these attacks is to listen to data that is trafficked over the network, and these attacks are often used to identify various possible vulnerabilities.

Active attacks are those in which the intruder engages in stealing messages, modifying them, deleting, running applications, changing content or addresses, redirecting, substituting, refusing a service, repudiating, etc. These are the most serious and dangerous because they can cause massive damage, with the most unpleasant legal consequences. Also included in this category are programs designed for destructive purposes that seriously, sometimes even catastrophically, affect the security of computers and information in general. This category includes: viruses, logical bombs, worms, hatches, Trojan horse programs, etc.

In accordance with (CISCO 2014) radiography reveals current cyber attacks:

a) Characteristics of current attacks

a1. Are more ingenious in taking advantage of existing gaps in the security system: in 2014, 1% of the most common vulnerabilities took advantage;

a2. Security of Java processing has increased by 34% in 2014 and attackers are expected to find new vulnerabilities through JavaScript;

a3. The volume of spam increased by more than 250% in 2014;

a4. A new spam technique (snowshoe spam) has improved, which not only makes it difficult, but sometimes makes it even impossible to detect the source.

b) Users along with IT teams have become part of the security system

b1. Current attackers rely on users to install malware or exploit security gaps;

b2. 56% of the OpenSSL versions are older than 50 months and are therefore still vulnerable;

b3. Uneven internet usage and access to unprotected web pages;

b4. Malware developers use web browser extensions as a means of distributing malware and unwanted applications.

c) There is no consensus on the perception of security among different categories of actors:

c1. 59% of security chiefs (CIOSs) say that it is optimized, as opposed to only 46% of security operators (SecOps);

c2. About 75% of CISOs perceive security tools as highly effective, while 25% consider them only partially and effectively;

c3. 91% of respondents from companies that have implemented a sophisticated security system claim managers give security a high priority;

c4. Only 50% of respondents use patches to repair mistakes or omissions of the systems they use;

c5. Medium and large organizations have more sophisticated security systems than other types of organization.

The most common types of attacks (**Table no. 1**) include: denial of service, viruses, worms and trojans, device theft, phishing and social engineering or web attacks.

Table no. 1: The main categories of cyber attacks

No.	Attack type	
1.	DoS (Denial of Service)	This category includes attacks designed to interrupt the normal operation of hardware and software equipment through the DoS method.
2.	Attacks on web applications	This category includes attacks through web applications.
3.	Cyber-espionage	This category includes attacks conducted with the objective of gaining unauthorized access to classified data for the purpose of espionage.
4.	Abuse in privileged access	This category includes attacks or incidents caused by inappropriate abuse or misuse of logical access rights to the organization's network, systems, data, and equipment.
6.	Payment card skimming	Payment card skimming This category includes attacks or incidents based on the implantation of a device on financial data reading equipment (eg ATMs, PoS terminals, etc.).
7.	Point-of-sale PoS attacks	This category includes attacks from remote access of data and financial transactions read through a card reader (such as PoS terminals), except in the cases included in the previous category.
8.	Cybercrime	This category includes attacks with any objective other than cyber-spying, and includes any techniques that can not be categorized into another category.
9.	Snowshoe spam	Involves sending small volumes of spam from a large set of IP addresses to avoid detection.
10.	Soft malware	Software that aims to damage or deactivate computers and computer systems.
11.	Errors	This category includes incidents whose cause can not be assigned to another category.

The impact of cyber attacks on the victim's organization, although impossible to quantify due to lack of information, most often causes loss of information, disruption of activity, compromise of confidentiality of information (data most often compromised including identification data such as address or PNP, medical information, phone, financial data, e-mail addresses, usernames and passwords, etc.), equipment damage or theft or potential revenue loss.

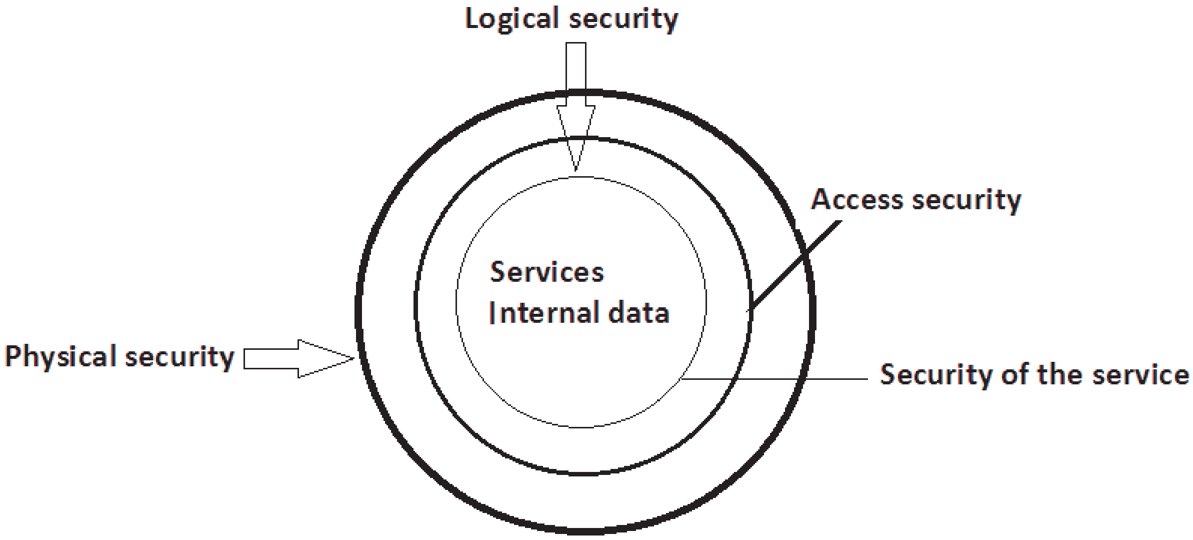
A careful look at the main causes that allow cyber attacks to succeed (Bendovschi, A., 2015) shows that in more than 50% of cases, the success of a cyber attack is only partly due to the attacker's expertise and skill, while allowing vulnerabilities in system frameworks, human error and / or insufficient level of security controls implemented. To support this conclusion, Cenzic detected at least one major vulnerability in over 95% of the systems analyzed in 2013, with an average of 14 vulnerabilities per application (Cenzic, 2014). Another very important result in the current research is that in at least 20% of the cases the attackers are not entirely foreign to the organization, among them business partners, former employees, etc.).

2. Information security

Computer security is now a vital issue for all computer system users, especially in the broader era of the Internet, whether they are service providers or are simple users. The growing need for communication, on the one hand, and information protection, on the other, are two different, if not even opposite, requirements.

The implementation of a modern security system in accordance with (Tăbuşcă, 2009) provides for protection on several levels (Figure no. 1).

Figure no. 1: Security levels



The first level is provided by *physical security*. Physical security generally consists of "locking" equipment, placing it in special rooms away from fire, weathering, physical destruction, whether intentional or not. It is a measure applicable to all computing systems, but less feasible in the case of networks, especially those of medium size, and even less of those with large area of spreading. The second level of protection is provided by logical security and includes the schema of methods for controlling access to system resources and services.

Logical security deals both with security of access, as a first sub-level, as well as security of services, sub-level that is "under" security of access in terms of security structure. **Access** security includes: access to the system, responsible for determining whether and when the system is accessible to users, and especially under what conditions. He is responsible for managing the access record. Access to the system can also force forced disconnection in certain cases (account expiration, peak time, etc.); verifying access to an account at the level of name and password validation; access rights (files, resources, services, etc.) that determine what privileges are available either to a user or group of users.

Service security is concerned with: controlling the services responsible for warning and service status reporting, as well as activating and deactivating the various services provided by the system; service rights that determine how a given service uses a given service (access to files, resources, priority, etc.).

Basically, once the logical connection is established, the access security subsystem validates access or not. The service security subsystem monitors user activity and takes action in cases where its requests exceed the rights specified in the user's profile. Access to a perfectly secure system should be done through these security levels, without being allowed to bypass any of them.

3. Mutations induced by automated data processing on financial accounting management and audit work

The main mutations induced by the use of highly computerized information systems on financial and accounting management (Oprea, D., 2008) refer to:

- Removing the traditional way of keeping documents and managing them - *more people can access the same data*;
- Concentration trend of data processing - *the risk of unauthorized loss or consultation increases*;
- The dominant principle of automatic data processing (P.A.D.) GIGO (garbage at the entrance - garbage at the exit) - *an error in an integrated system propagates rapidly*;
- Additional requirements for those in charge of data protection who: - can not understand the ways in which data can be accessed in secret (for stealing or modifying) *or fail to detect where and who has remote unauthorized access*;
- P.A.D. changes information support and means of work and protection: *increases the density of information* - easy to hide; obs*curity or invisibility of information* - can not be visually notified; *very easy accessibility* - new categories of criminals; *lack of traceability* - modification or addition of new, easy to make and hard to find data; *retention of media* - deleted data can be recovered; *data aggregation* - can reveal vital elements.
- Not knowing the computer - *is overwhelmingly confident*;
- Technological progress in accessing data increases but not in their security;
- Strong integration of systems - has increased appetite for *fraud* and facilitates the proliferation of *errors*;
- Processors are very vulnerable to hardware specialists - *modify* the registry and use privi*l*eged instructions;
- Communication facilities - serve as a means *of fraud* by intercepting the transmitted signals;
- Remote terminals can be *controlled and hijacked* by special devices;
- The more complexity increases, the greater the risks.

4. Risks in financial audit activity and risk attitude in cyber attacks

Professional judgment in the audit is exercised in a context of risk (Gray and Manson, 2005). The idea of risk and insurance has been present in the economy and business since the beginning of the period when man began commodity exchanges. The process of globalization, the economic crisis triggered in 2007 and increasingly frequent cyber attacks have made the risk of gaining new valences, being more diversified in nature, and being approached more by any economic entity. Although the notion of risk is unanimously accepted, it is accepted that the risk relates to unpredictability, decision-making and potential loss. The risk is related to the decision-making process (March and Shapira, 1987), and any decision taken in the economic field in general and in business in particular involves some degree of risk. Faithful image and significant misstatement are assessed in the auditor's professional judgment based on risk. Kendrick (2004) emphasizes the importance of understanding personal attitudes about risk, and believes that attitudes and risk behaviors are key dimensions in understanding risk. The attitude of risk decision makers in cyber attacks can be assessed by the level of top management involvement in deploying complex security systems.

At the level of an audited economic entity, the audit risk in general is manifested through its basic components: **inherent risk, control risk and non-detection risk**, and can be determined both in quantitative terms (in percentages) and in qualitative terms (*risk low, moderate, high or very high*).

Given the risks of cyber attacks on audited information systems, the quality level of security systems and **the level of security risk** should be assessed.

To assess the quality of security systems and to quantify the level of security risk there are many concerns in the world of specialists. One of these is provided by the Mehari, a registered trademark of CLUSIF (club de sécurité de l'information française), which provides: bets analysis guides, security assessment, and security risk analysis. Among the practical facilities offered, Mehari provides its own knowledge base that allows quantification of the quality level according to the implemented or non-implemented activities (controls). Quality levels defined by the Mehari method in increasing order from 1 to 4 are characterized by the fact that, for example, Quality Level 4 service: will remain active against all aggressions - could be broken in exceptional circumstances by the best code breakers in the world with the best tools. Under these circumstances, the risk is determined by the Mehari method as the difference between the maximum *level of quality 4* and the average level of security quality determined on the basis of a complex investigation of the security system.

Based on a study conducted with the help of 60 master students at the CAIG (Auditing and Management Information Management) in the years 2016-2017 at the companies they worked or worked on, a 2.73 average quality was achieved and therefore an average quality risk level of 1.27.

The main three deficiencies found on each security domain are summarized in Table no. 2.

Table no. 2: Three deficiencies noted in each area security

Domain	Incorrect or incomplete activities implemented
1. Organization of security	**No** classification of the information (documents, data, files, databases, etc.) has been performed depending on the impact of a disaster that could affect this enterprise information.
	There is **no** clause in the employment contracts or in the internal regulation which specifies the obligations to observe the set of security rules in force.
	The risks associated with third-party access (suppliers, customers, investors, etc.) have **not** been analyzed in the information system or in the sites containing information and the necessary security measures have not been established.
2. Site security	There is **no** procedure to allow for subsequent detection of irregularities in the management of access authorizations (badge or book not returned, lost, false, etc.).
	There is **no** system in which to ensure that the same badge can not be used by a second person (eg by storing all entries and not allowing an extra entry without a previous exit)
	Not all possible access ways are monitored in addition to normal access control, access via other routes (such as outside accessible windows, emergency exits, false floorings or ceilings).
3. Security areas	There is **no** power control system that includes at least one uninterruptible power supply for the most sensitive equipment.
	Electrical circuits and cables are **not** protected by surge and lightning equipment.
	No inventory or classification of all types of sensitive locations has been made.
4. Extensive networks	It is **not** checked whether the use is made in accordance with the configuration and the need for user use.
	There are **no** sufficiently effective penalizing clauses on the quality of services provided by the service provider.
	Disaster recovery solutions are **under-exercised**.

Domain	Incorrect or incomplete activities implemented
5. Local network	The local network was **not** partitioned into security domains, each requiring a set of security rules, or in trusted areas where controls are specifically tailored.
	There is **no** procedure for handling inter-domain connection requests and a group to deal with the analysis of these requests, with their authorization and the definition of filtering rules to be implemented (firewall, service requests, protocols , etc.).
	No systematic analysis of potential single failure points has been carried out to ensure that service equipment (such as power, air conditioning, etc.) does not affect the planned redundancy of network equipment or network architecture.
6. Network Operations	There is no security policy directed at staff operating on the network covering all aspects of information security (information confidentiality, availability of information and services, integrity of information and configurations, ability to track operations, etc.)
	It is **not** mandatory for all maintenance operations to end with a systematic check of all security parameters (as defined at start of implementation).
	The system configuration integrity is **not** regularly tested according to the expected theoretical configuration requirements (at least weekly, if not every time the system is activated).
7. Systems architecture and logical security	There is **no** regular audit, at least once a year, of the set of rights assigned to each profile and profile management procedures.
	There is **no** systematic updating of the authorization table when changing the function.
	The process of assigning or changing user IDs does **not** comply with a set of rules that ensure their intrinsic validity. In the case of passwords: adequate length (8 characters or more), mandatory mix of different character types, frequent change (at least once a month), the impossibility of reusing old passwords, banal words, nicknames, names anagram, personal data, easy to find, etc.
8. IT Production Environment	These are **not** the same mandatory clauses for entrepreneurs working with operating systems as for internal staff.
	There is **no** routine check to verify if the rights of the personnel managing system operating systems have changed which could trigger an alert if this happens.
	Reference documents are **not** protected by secure methods, against premature or unlawful modification.
9. Security of processing	There is **no** procedure detailing the actions to be taken in the event of an error or alert.
	There is **no** one or more applications capable of analyzing individual data diagnosed with anomalies and triggering an alert to operational personnel.
	There are **no** mechanisms for stopping recording and processing of recordings when an alarm is triggered.
10. IT projects and security development	There are **no** studies and reviews of the new project presenting the risks, the decisions taken on whether or not to accept it, and any additional necessary security measures.
	Upon the purchase of a new application, there is **no** guarantee that the competence and availability of the supplier's maintenance staff allows them to respond satisfactorily to user maintenance requests. This agreement should take into account the weekend and holiday times as well.
	When developing a confidential application, profiles are **not** established to allow confidential information to be shared so that access to them is restricted to people who have a real need.
11. Managing user workstations	Control procedures related to user configuration are **not** subject to periodic auditing.
	The compliance of workstation hardware configurations is **not** regularly checked against authorized options.
	The IT department does **not** manage a reference for each software installed on user workstations (source and executable code).
12. Telecommunications operations	There is **no** regular audit, at least once a year, of the effective implementation of the assessment, signing and resembling procedure by the operational staff (directly or indirectly employed by a service company) of the security obligations.
	Security measures designed to counteract the identified new risks are **not** formally reviewed before implementation.

Domain	Incorrect or incomplete activities implemented
	Service contracts do **not** detail the required time intervals and days of intervention that are compatible with availability requirements.
13. Management processes	The **PPI** (Personal Information Protection) Directives do not cover all legal obligations, including those relating to the collection, access, communication, use, storage and destruction of such information.
	There is **no** committee attached to government bodies responsible for developing financial data communication and regularly studying and solving different issues.
	Nu se realizează evaluări periodice care vizează nivelul de cunoaştere a personalului cu privire la protecţia sistemelor informatice şi a mecanismelor de securitate.

Conclusions

Given that cyber attacks have increased year by year and computer system users have become facilitators or accomplices from targets, the popularization of the main mechanisms to make these attacks is not only necessary but even mandatory. The auditor, when auditing the activity of a highly computerized entity, in the audit risk assessment, along with its core components: i**nherent risk, control risk and non-detection risk** must introduce a new component **specifying the level of security risk**, without which a quality audit can not be achieved. În condiţiile în care atacurile cibernetice au crescut an de an şi utilizatorii sistemelor informatice, din ţinte au devenit facilitatori sau complici, popularizarea principalelor mecanisme de realizarea a acestor atacuri este nu doar necesară ci chiar obligatorie.

BIBLIOGRAFIE

1. Bendovschi, A. (2015), Cyber-attacks – trends, patterns and security countermeasures, *Procedia Economics and Finance,* vol. 28, pp. 24-31, DOI 10.1016/s2212-5671(15)01077-1.
2. Gray, I., Manson, S. (2008), *The audit process: principles, practice and cases*, Thomson Learning, UK, London.
3. Kendrick, T. (2004), Strategic risk: Am I doing OK?, *Corporate Governance*, vol. 4, nr. 4, pp. 69-77, DOI 10.1108/14720700410558899.
4. March, J.G. and Shapira, Z. (1987), Managerial perspectives on risk and risk taking, *Management Science*, vol. 33, pp. 1404-1418, DOI 10.1287/mnsc.33.11.1404.
5. Oprea, D. (2008), *Protecţia şi securitatea informaţiilor*, Iaşi, Polirom.
6. Tăbuşcă, A. (2009), A quick look at the future of protection – nine guidelines to follow, *Journal of Information Systems & Operation Management*, vol. 1, nr. 3.
7. CISCO (2015), *Annual security report 2015*, disponibil la https://www.cisco.com/c/dam/assets/global/DE/unified_channels/partner_with_cisco/newsletter/2015/edition2/download/cisco-annual-security-report-2015-e.pdf, accesat la data de 1.11.2017.