12

Frauds and Information Technology: Analysis of the Influence on Accounting and Company Systems

Jacqueline Veneroso Alves da Cunha
Edgard Bruno Cornachione Jr.
University of Sao Paulo (BRAZIL)

Abstract: In an age characterized by information technology, this article aims at criticizing, pointing out and discussing some considerations about frauds in the organizational and more specifically the accounting and company information systems environment. First, the subject will be conceptualized and characterized, discussing the different existing forms and techniques for committing fraud. Then, we will treat a crime that is very common nowadays and that has been causing constraints and great damages to the corporate world, namely, the frauds realized in/with computers. Frauds have always occurred within companies, but the development of information technology provided them with such a speed and refinement they did not have before, which is aggravated by the fact that these crimes are difficult to detect.

Keywords: frauds, internal controls, employees, financial statements, opportunity, computers, information technology, computerized frauds and audit.

1. INTRODUCTION

The world is going through a changing process characterized by the increasing flexibility, approximation and virtualisation of markets, organizations and products, which are largely provoked by Information Technology and globalization. This technology allows for connections all over the globe, turning business, information and decision processes more agile. Nevertheless, technological development and globalization have not only caused benefits for the organizations. Besides, they have also opened fertile ground for the dissemination of a white-collar crime called "fraud", which is being realized in and with computers nowadays.

The influence of these changes has already reached the entrepreneurial environment. The easy use of the computer machines and the potential of

programming languages, allied with the high and increasing number of connections spreading out all over the planet, allow for a fast access to information, which can be used in a fraudulent way.

This fact, together with the commodity and safety of the defrauder for not being obliged to be physically present at the place of the crime (less exposure), are definitely the main factors responsible for the fabulous increase of this kind of crime within organizations.

Formerly, any invasion or espionage demanded the participation of the human being at the specific place of the fraud. Nowadays, the rules are different. Computation, electronics and telecommunications have transformed this reality. People and companies all over the world no longer need to send "spies" to perform criminal acts, although various kinds of fraud still depend on the presence of an insider within the company. This article proposes a contribution to the knowledge of the characteristics, circumstances, objectives and patterns of frauds and defrauders. Allied with good internal control, these serve as a means of trying to alert companies and make them prepared to anticipate this kind of crime.

2. REVISION OF FRAUD CONCEPTS AND CHARACTERISTICS

Considering various interpretations of what constitutes fraud, all of them highlight actions such as threatening, fooling, forging, deceiving, tricking, misleading, whether intentionally or not. According to CAMBRIGDE [1], fraud is *"the crime of obtaining money by deceiving people"*. For FERREIRA [2], it is *"abuso de confiança: ação praticada de má-fé"*. PARENTE *apud* SOARES [3] considers it *"uma quebra proposital das ligações existentes entre a realidade e a sua representação manual ou automatizada, com o fito de se obterem vantagens direta ou indiretamente"*.

To ROMNEY, STEINBART and CUSHING [4], fraud *"is any and all means a person uses to gain an unfair advantage over another person"*.

[1] CAMBRIDGE, *International Dictionary of English*. London: Cambridge Press, 1995. p.559.

[2] (transl.) "betrayal of confidence: an action practiced perfidiously". FERREIRA, Aurélio Buarque de Holanda. *Novo Aurélio século XXI: o dicionário da língua portuguesa*. 3. ed. Rio de Janeiro: Nova Fronteira, 1999. p. 940.

[3] (transl.) "a deliberate breach of the existing links between reality and its manual or automated representation, aimed at obtaining advantages directly or indirectly". SOARES, Antonio de Pádua. Sistemas eletrônicos de dados como fator preponderante na evolução da auditoria convencional. Monograph for obtaining the title of specialist in Accounting Consultancy. Belo Horizonte : Unicentro Newton Paiva, 2000. p.45.

[4] ROMNEY, Marshall B., STEINBART, Paul J., CUSHING, Barry E. *Accounting information systems*. 7. ed. USA : Addison-Wesley Publishing Co., 1997. p. 503.

Broadly speaking, then, fraud can be conceptualized as any means used by a person or institution aimed at obtaining an unjust advantage over another person or institution whether by act or omission, by means of intentional behavior or perfidiously. That is, fraud is made up by doing as well as by omitting to do something, whether this behavior is intentional, not necessarily aimed at impairing somebody, or perfidious, when the intention is fraudulent or criminal.

2.1 Kinds of fraud and Defrauders

The variety of means used by a defrauder depends on the objectives he wants to reach. These can consist of lies, tricks, and omissions of the truth, among others. It also depends on whether an insider or outsider to the entity will commit the fraud. The controls used by companies to protect their possessions are expected to difficult the action of external defrauders. An insider to the organization, however, knows internal policies and procedures, which makes it easier to commit and hide a fraud, whether alone or with the help of other insiders to the entity. When the defrauder receives help from other people, he needs to surmount obstacles to his safety beyond his position, resulting in a higher level of exposure. In accordance with ROMNEY, STEINBART and CUSHING [5], internal fraud can be divided into two categories: fraud by the employee and fraud in financial statements. In case of fraud by the employee, committed by a person or group of persons for private financial gain, the defrauders can be divided into three groups, conforming LEVI *apud* SOUZA [6]:

a) Pre-planned defrauders – are those who start committing fraud with pre-established goals, developing schemes, like for example obtaining a higher-level job within the entity to commit fraud.
b) Intermediary planning defrauders – are those who start their career with honest intentions, but any other motives, such as excessive personal spending provide the impulse to commit fraud.
c)Occasional defrauders – are those who never had the conscious intent to commit fraud, although circumstantial problems like bankruptcy of the company, unsettled debt and bad management of financial resources turned the entity or person insolvent. An occasion could also be such a situation where and when the fraud is easy to commit, like non-secure information systems.

Fraud in financial statements, whether committed intentionally or perfidiously, results in false statements, which are used for making a company's share price increase or decrease to attend to cash flow needs, hide

[5] *Op. cit.* p. 503.
[6] SOUZA, Fernando de Jesus. *Perícia contábil e prevenção de fraude.* Revista Perícia Federal. DF : APCF, 1, 03/1999. p. 22.

company problems, deceive investors and creditors, or for fiscal purposes. In this specific case, the defrauders obtain an indirect benefit, whether through the maintenance of their employees or for the purpose of salary increases and promotions. According to this, the report by Peat Marwick Thorne, Inc. (KPMTG international fraud survey report. Toronto, 1993), quoted by NEPOMUCENO [7], classifies fraud in three categories: fraud by employees, fraud by managers and external fraud.

2.2 The Process of a Fraud

Most of the fraud processes involve three stages, as stated by ROMNEY, STEINBART and CUSHING [8]:

a) In the first stage, some value is actually stolen, whether represented by money, inventories, tools, machinery or data. In case of employee fraud, it generally involves some asset while, in case of financial statement fraud, it generally involves over/under valuation of assets.
b) In the second stage, in case of inventories, tools or equipments, the stolen assets are converted into money (they are sold or transformed into money in another way).
c) In the third stage, the crime is hidden so as to avoid being discovered and arrested. This demands most effort and time, since it can leave tracks that evidence the actual crime. Getting money only takes some seconds, but hiding the act takes more time, ability and challenge.

Considering this 3-step model it is easy to figure out that one relevant aspect of computer fraud process is quite related to planning. Therefore, defrauders spend time analyzing and testing the systems, searching for weak controls or special opportunities. Thus, the computer fraud process is more intense regarding planning due to its own nature. But, a computer crime can generate a leak of millions of dollars within just few seconds.

2.3 The Motive for Fraud Occurrence

Defrauders are called "white-collar" criminals, and are differentiated from those criminals who commit violent crimes, as they do not present big threats for the public in general. In accordance with ROMNEY, STEINBART and CUSHING [9], some of the defrauders' characteristics are: they do neither invest nor save the illegal income, but merely spend it; after they have started, it is difficult for them to stop the fraud; they usually depend on the extra income; the desire for more money makes them take

[7] NEPOMUCENO, Valério. *O positivo e a neutralidade contábil.* Revista do Conselho Regional de Contabilidade do Rio Grande do Sul. Porto Alegre : 105, 08/2001. p. 21.
[8] *Op. cit.* p. 504.
[9] *Op. cit.* p. 505.

away more and more; over time, they become more confident and careless, which leads to their arrest; most of them do not have a previous criminal record; before they committed the fraud, they were honest and respectable citizens. Many are dissatisfied and unhappy at work, which makes them seek to obtain more from their employer. Others are considered perfect and dedicated employees who work hard and occupy positions of trust.

ROMNEY, STEINBART and CUSHING [10] indicate three motives that make people commit fraud:

a) Pressure: Can be financial, when the individual lives beyond his means or is heavily indebted. It can also be related to work, or provoked by resentments, mistreatments, low salaries or the feeling that his talents are not recognized or are being exploited by the company. Besides, it can be provoked by family, emotional instability or even the challenge to defeat the dominant system, which is more common in computer fraud.

b) Opportunity: Is that condition or situation that allows the individual to commit and hide a dishonest act. This opportunity can arise from the failure or inexistence of internal controls, incompetent supervisors, an excess of confidence in key employees, a lack of attention to details or through personal relations with clients and/or suppliers that become mutually advantageous. Fraud also reveals a tendency to occur when some crisis appears and the company temporarily neglects its standard internal control procedures.

c) Rationalizations: It is the reason that allows the "white-collar" defrauder to excuse himself or justify his illegal behavior. The argumentation is that he is not hurting anybody, since only a company without name or face (impersonal) will be affected, that the embezzlement will get him out of a situation that will not last long, so he is not being dishonest, since he intends to give back the money as soon as possible. Or that the company owes him this for his good service; in this case, he is only taking what is his by right. It is also called the "Robin Hood Syndrome" (acting for a good cause); "I occupy an important position so I stand above the rules", or even, "what I did is not that serious since everybody is doing it and you would understand if you knew how much I needed it".

3. FRAUDS IN COMPUTERS

"In 1966 a programmer working for a bank had an overdrawn bank account. (...) He meticulously programmed his IBM 1401 computer to ignore his $300

[10] *Op. cit.* p. 506-08.

> *overdraft, intending to replace the money three days later. (...) Four months later, he had increased this amount to over $350. He was caught when the computer broke down, thus earning him the dubious honour of becoming the world's first known computer criminal."*[11]

Computer fraud is defined by the American Justice Department as *"any illegal act for whose perpetration, investigation or condemnation, the knowledge of computer technology is essential"* [12].

Computer fraud can go from children's play to industrial espionage. Money embezzlement is the most common form, although fraud can involve services, information or programs, the use, copy, change or destruction of software or unauthorized data, among others. Some studies have been made to determine the computer crime categories and their frequency. One of these studies [13] highlights over 30% due to "service theft", 35% to "money theft" and the third place is due to "information theft" (over 10%).

Considering that, through the use of computers, the defrauders are capable of doing much more harm in much less time without leaving hardly any evidence, it is much more difficult to detect this kind of fraud.

The big difference between the computer fraud of the digital age and other "white-collar" frauds lies in the fact that, in the case of computer fraud, the virtual criminal no longer needs to be physically present at the place of the crime. Digital crime can be practiced in and from the most different places all over the world.

The faster access to remote computers and the increasing number of users have transformed computer fraud into a freely expanding industry. However, technology advancements do not only cause benefits for society as a whole.

Global connections through the global network that, according to NOGUEIRA [14], *"são mais de 500 milhões de usuários e U$ 40 bilhões em transações"*, also allow for the dissemination of frauds in record time. ROMNEY, STEINBART and CUSHING [15] present some data as follows:

a) The FBI estimates that only 1% of all computer crimes are detected;
b) The National Center for Computer Crime Data concluded that the average loss per computer fraud amounts to US$ 109,000;
c) Between 50% and 90% of the companies lose money through computer fraud, in accordance with studies by Ernest and Whinney;

[11] MOSCOVE, Stephen A., SIMKIN, Mark G., BAGRANOFF, Nancy A. *Accounting information systems: concepts and practice for effective decision making*. 4. ed. New York/USA: John Wiley & Sons, 1990. p. 381.

[12] *Op. cit.* p. 508.

[13] *ROMNEY, STEINBART and CUSHING, Op. cit.* p. 510. *Adapted from Michael Alexander,* "Computer crime: ugly secret for business", *Computerworld, 1990. p. 104.*

[14] (transl.) "accounts for more than 500 million users and U$ 40 billion in transactions". NOGUEIRA, José H. Matos. *A nova face do crime*. Revista de Perícia Federal. DF: APCF, 9, 07/2001. p. 14

[15] *Op. cit.* p. 509.

d) The Bank Administration Institute pointed that American banks lose more than U$ 1 billion per year due to information system abuse.

And also, according to data from Carnegie Mellon University [16], in the United States, the amount of hacker attacks grew by 150% in 2001.

In Brazil, according to the Federal Police Department-DPF [17] the organ responsible for repressing this kind of crime, only 214 (1%) out of 21,161 reports made by the National Crime Institute (INC) and by the Criminology Sections (SECRINs) in 2000 were computer fraud reports. According to NOGUEIRA [18], in Brazil, the first public contest for experts specialized in informatics was only made in the department in 1993. Some time afterwards, the first Computer Crime Combat Section (SECC) was created; some public safety organs have been creating sectors and police stations specialized in computer fraud, like in the case of the civil police in Brazil (São Paulo and Distrito Federal) but, until now, a specific legislation for this new kind of crime is still lacking. Although some law projects have reached the National Congress, they are paralyzed and without any perspective of a fast approval.

Nevertheless, the actual hole provoked by computer fraud is not known, considering that estimations are only based on the reported and detected frauds, and many of them are not, since companies are afraid that negative publicity will cost more than the fraud in itself and, also, since many people do not believe that making an unauthorized copy of a software is a crime. So [19], *"(...) we can only consider the presently known cases of computer crime a sample, rather than a population, of modern computer abuse"*.

3.1 Profile of the Computer Criminal

Quoting MOSCOVE, SIMKIN and BAGRANOFF [20] on the profiles of the computer criminal:

> *"Of course, it is not always possible to construct a profile for a given type of crime. In the case of computer crime, however, there appears to be a remarkable number of similarities among the individuals who have been caught using a computer illegally."*

Superior knowledge – computer criminals tend to be brilliant, talented and qualified, with a good intellectual level and higher education and are normally younger than 30 years – the fact that younger people frequently have greater financial needs and are more willing and wanting to take risks may contribute to this.

[16] MOURA, Betina e HORTA, Ana Magdalena. *Uma terra de piratas*. Revista Época. São Paulo : Globo, year IV, nº 199, p.84-89, 11/03/02. p. 84

[17] Data from the Report Production Map per month/year by the National Institute of Criminology of the Federal Police Department in 2000.

[18] *Op. cit.* p. 18

[19] *Op. cit.* p. 385.

[20] *Op. cit.* p. 400.

Morals – most of the computer criminals consider themselves to be relatively honest people who borrow things on a long-term basis and do not see themselves as criminals, taking great care not to damage any individual by their illegal actions.

The challenge of defeating the system – this attitude tends to remove the criminal stigma from illegal computer activities, characterizing computer crime more as a game than as a violation of moral conduct.

Non criminal base – few suspects arrested for computer crime possess a previous criminal record, they are amateurs and primary criminals.

Environment – computer criminals need an opportunity to commit crime.

ROMNEY, STEINBART and CUSHING [21] also synthesized the characteristics that make up the computer criminal profile, highlighting computer experience and ability, motivation by the challenge of defeating the system more than by actual gain and the tendency to be younger and consider their actions as a game and not as a crime, which actually confirm the characteristics accentuated by the previous authors.

3.2 Computer Fraud Techniques

There exist many kinds of fraud and many ways in which the computer can be used for committing them or being their target. The simplest and most common way is to commit a fraud by changing computer inputs. There is no need for great ability, merely some operational system knowledge. A defrauder can change his own salary, for example, create a fake employee to receive his remuneration or also deviate or make bad use of the outputs realized by means of monitors or printers.

Among the most common listed techniques for committing computer fraud, we can quote:

a) Round off figures downwards, when the programmer instructs the computer to round off calculations downwards. The fraction of a cent generated in each calculation is placed in his own account.
b) Software piracy, which is its illegal copying. It is estimated that, for each legal copy, between one and five illegal copies are made.
c) Breach of data, which is the illegal copying of company data, e.g. its client list.
d) Hacking, which is the unauthorized access and use of computer systems, usually by means of a personal computer and a telecommunication network. This technique is very common nowadays and its criminals, called hackers, are all over.

In accordance with NOGUEIRA [22]:

[21] *Op. cit.* p. 505.

[22] (transl.) "Over time, different variations of a hacker have appeared. Depending on the purpose of his acts, he can be called other names. Although there does not exist any

> *"Com o passar do tempo têm aparecido diversas variações do que vem a ser um hacker. Dependendo da finalidade de sua atuação, ele pode ser conhecido por outras denominações. Apesar de não haver consenso entre os autores, vale a pena diferenciar esta nomenclatura apenas para facilitar a terminologia empregada no meio (e.g.: Hacker, Cracker, Phreaker, Wannabe, Lamer, Sneaker, Wizard)".*

In the last edition of a global competition (August 2001), the evaluators, represented by experts, elected a Brazilian of 26 years old and born in Rio de Janeiro as the biggest hacker in the world. He is the three-time champion in system hacking and accumulates victories in championships promoted by the SANS, one of the five biggest safety institutions in the world. In the last test, he spent 15 minutes to get into a network considered safe, competing with 1500 other specialists.

Nowadays, the champion works in the biggest safety company in Latin America: Módulo. In most cases, the Brazilian hackers use their abilities on national pages. This is proved by the fact that the sites ending in "dot br", occupy the second place in the global hacking ranking. They are only preceded by the "dot com" sites.

3.3 Detaining and Detecting Computer Frauds

Starting from the premise that it is practically impossible to eliminate any kind of fraud definitively, we must attempt to decrease the risk of their occurrence, resorting to preventive measures.

It is clear that no measures can prevent all cases, but people as well as entities can learn from past happenings, decreasing a lot the risk of re-occurrence.

However, according to a research realized by Módulo Security Solutions [23] with 165 businessmen from public and private companies, 31% of them did not even know whether they had been attacked, and 40% had already been the target of hackers going through their documents, and 29% stated that never suffered an attack.

Some measures significantly decrease the possibility of fraud and the resulting losses. Among these:

a) Create a climate less inclined towards fraud: presupposing that most frauds are committed by current or previous employees, companies can adopt procedures that stimulate the integrity of the employee, his compromise with the company and reduce the inclination towards fraud commitment. Measures like: employee training; management of dissatisfied employees; contracting and dismissal ability; education

---

consensus between the authors, this terminology must be differentiated merely in order to facilitate the terminology used in the field (e.g.: Hacker, Cracker, Phreaker, Wannabe, Lamer, Sneaker, Wizard)". *Op.* cit. p. 16.

[23] MOURA, Betina e HORTA, Ana Magdalena. *Op. cit.* p. 85

directed by the promotion of its ethical standard, among others, would help the company to maintain a greater control of a vulnerable point.

b) Increase the difficulty to commit fraud: deals with decreasing the opportunity of fraud occurrence. This becomes possible through the creation of an internal control system and the follow-up of its execution. Among some kinds of internal control that bring about results, we have: segregation of functions and obligations; holidays with task substitution and turnover; restricted access to computer equipment and data files; protection of phone lines (as a way of protecting against hackers); protection of the system against viruses.

c) Improve the fraud detection system: the sooner the fraud is detected, the faster the procedures to detain it can be put in practice. Some steps can be adopted to detect a fraud as soon as it is established. They are: conduct periodical internal and external auditing; maintain a computer safety representative; create an anonymous fraud denouncement line; maintain informatics consultants; monitor system activities; reveal and punish defrauders.

d) Reduce losses caused by fraud: since the chances of fraud occurrence do not end, but merely decrease, the company should prepare itself in order to minimize the losses resulting from fraud occurrence through the maintenance of adequate safety, the use of system activity monitoring software, the development of a contingency plan for fraud occurrence and the keeping of updated copies of all files, programs and data in a safe place.

Protection spending has increased. In Brazil, it jumped from R$ 68 million in 2000 to R$ 85 million in 2001 [24]. But the losses provoked by attacks are still enormous. In 2001 it was possible to note the rise of losses under R$ 50.000,00, over 90% (in 2000 it was near 60%).

4. FRAUD AND ACCOUNTING

Initially, a distinction must be made between accounting fraud and accounting errors. In Brazil, the Federal Accounting Council [25] makes the following distinction:

> *"11.1.4.1 – Para os fins destas normas, considera-se: a) fraude, o ato intencional de omissão ou manipulação de transações, adulteração de*

[24] MOURA, Betina and HORTA, Ana Magdalena. *Op. cit.* p. 89

[25] (transl.) "11.1.4.1. – For the sake of these standards, it is considered that: a) fraud is the intentional act of omitting or manipulating transactions, adulterating documents, records and financial statements; and b) error is the unintentional act that results from omission, carelessness or wrong interpretation of facts when elaborating records and financial statements." CONSELHO FEDERAL DE CONTABILIDADE – *Normas Brasileiras de Contabilidade* : NBCT-11, Da auditoria contábil, 1999.

> *documentos, registros e demonstrações contábeis; e b) erro, o ato não intencional resultante de omissão, desatenção ou má interpretação de fatos na elaboração de registros e demonstrações contábeis."*

Consequently, accounting fraud is committed with the intention of impairing somebody, while the accounting error does not have the same objective. Fraud always occurs when a premeditated error is committed against third parties.

In accordance with SÁ [26], there exist victims and agents of accounting fraud. These include the company, the shareholder or partner, the company administration, the supplier, the client, the bank, the government, the employee. Consequently, employees can commit accounting fraud against their company; companies against the government or against the market; an employee against the government, among others, exchanging the position of victim and agent. In general, accounting fraud is the result of opportunity and an adequate internal control makes its occurrence more difficult. Besides, knowing the different modalities of fraud that exist is an efficient protecting measure against them.

Enforcing internal controls is a major procedure against frauds. For instance, ROMNEY, STEINBART and CUSHING [27] state some major internal control factors (beginning with failure to enforce internal controls): lack of proper procedures for authorizations; no separation of transaction authority from custody; no independent checks on performance; no separation of accounting duties; lack of clear lines of authority; lack of frequent reviews; inadequate documentation; no background checks.

Moreover, due to the already discussed nature (planning) of computer fraud, it is better to prevent it with strong previous actions and efforts.

The most common accounting frauds occur in: cash movements, through embezzlements that are normally realized by employees; the omission of income and increase of expenses, which are practiced by the entrepreneur for impairing shareholders or tax authorities; the movement of inventories, through their under or overvaluation, in order to cheat on tax authorities as well as lenders; receivables, committed by the employee who receives and puts the cash in his pocket; permanent assets, committed by the company with a view to evading taxes (mainly Income Tax) or deceiving shareholders; liabilities, through the omissions of debts or their fictitious liquidation, and mainly in fictitious liability, which consists in maintaining a debt as "payable" in the liabilities, although the money has already been liquidated; and also equity fraud and fiscal fraud. Various ways exist for the undue use of accounting to commit fraud, but in accordance with SÁ [28]:

[26] SÁ, Antonio Lopes de. *Fraudes contábeis*. Rio de Janeiro : Tecnoprint, 1982. p. 16-19.

[27] *Op. cit.* p. 507.

[28] (transl.) "In order to detect and avoid fraud, there exist accounting methods of high technological value. (...) Accounting can be used to commit fraud as well as to avoid it". *Op. cit.* p. 18

> *"Existem métodos contábeis de grande valor tecnológico para detectar-se e evitar-se a fraude. (...) Assim como se pode 'usar' a Contabilidade para 'fraudar', pode-se, também, usar a Contabilidade para evitar-se a fraude".*

5. ACCOUNTING AND COMPANY FRAUD IN THE AGE OF INFORMATION TECHNOLOGY

The value of information technology development for corporate accounting systems lies beyond discussion. It increased the speed of data processing and gave agility and opportunity to the provision of information for decision-making, that is, levering company processes.

This sofisticated computarized environment improves business process while offers special opportunities to defrauders. Within this environment the fraud is difficult to detect and allows one to steal more in even less time.

Frauds can occur in any of the main aspects of a system (input, processing and output). For this reason we can find several auditing approachs: around the computer, through computer, with computer etc.

In addition, the main information technology segments (hardware, software, data base and telecommunication) are targeted by defrauders dealing with computers or peripherals destruction, software or data destruction, data records modification, network invasion etc.

According to ELLIOT and JACOBSON *apud* GELBCKE et all [29]:

> *"(...) A TI está transformando a maneira que os dados são gerados, armazenados, transmitidos, acessados e interpretados. Pode-se fazer mensurações e emitir-se relatórios oportunos, acurados e analíticos (...)"*

The effective use of all of the technology made available, however, exposed accounting to the misdeeds of computer fraud. According to MOSCOVE, SIMKIN and BAGRANOFF [30]:

> *"Computers tend to concentrate the asset-bearing information of an organization into a compact, but highly vulnerable, format. An accounting information system exploits this format for efficiency in data gathering, data processing, data storage, and data dissemination. The cost-effectiveness of such an accounting system begins to diminish, however, if it is unprotected and abused. Thus, an understanding of computer crime and its deterrents is an important control for accounting information systems."*

Therefore, if a corporate accounting information system reveals to be unprotected and subject to fraud, which is occurring much faster now, accounting loses its greatest use, that is, providing safe and timely

[29] (transl.) "(...) information technology (IT) is transforming the way in which data are created, stored, transmitted, accessed and interpreted. Things can be measured and adequate, accurate and analytical reports can be issued (...)"
GELBCKE, Ernesto Rubens et all. Assurance Services: novas oportunidades para a profissão. Boletim do Ibracon. São Paulo : nº. 248, 01/1999. p. 4

[30] Op. cit. p. 381.

information for its various users. In this way, the efficient and recurrent use of internal controls, together with other prevention measures that have already been dealt with, is the most efficient way of maintaining corporate information systems safe since, according to SÁ [31] *"O fraudador quase sempre testa os controles antes de praticar o seu ato doloso"*.

In the age of information technology, company fraud still results mainly from mistakes in the internal controls of organizations. The KPMG – Stokes Kennedy Crowley report, quoted by SOUZA [32], informs that 52% of the observed fraud cases result from the lack of internal control and of the establishment of a reconciliation procedure. As a result of the technological evolution, the difference is that they occur faster and easier, are easier to hide, and allow the defrauder to realize them outside the corporate environment. Organizations must adapt themselves to these new times, "*adaptação é o ferramental de convivência com o processo de mudança do negócio para atender o equilíbrio dinâmico do ambiente externo*" [33].

6. CONCLUSION

The environment organizations are inserted in is undeniably characterized by Information Technology and globalization, promoting large-scale development without any of the usual barriers known. There are two aspects to this advancement: 1) provides companies with the benefit of accompanying the entire evolution without deviating from the competitive race and 2) exposes the companies to the misdeeds of this development. Here, an old enemy appears in new clothing: fraud.

Although fraud has always occurred in the organizations, nowadays, it occurs in other forms and ways, at the speed of light. All of the technology available to serve the "good cause" can be used to cheat or steal.

Within the companies, one kind of fraud is the fraud practiced in corporate and accounting systems. Since accounting maintains the control of all of the companies' possessions, it constitutes a great attraction for the defrauders. Whether they are willing to embezzle assets, data or information,

[31] (transl.) "The defrauder almost always tests the controls before committing his fraudulent act". *Op. cit.* p. 26.

[32] SOUZA, Fernando de Jesus. A busca da evidenciação contábil em ambiente computadorizado. Revista Perícia Federal. DF : nº. 3, 10/1999a. p. 35

[33] (transl.) "adaptation is the tool for living together with the process of changing business in order to attend to the dynamic equilibrium of the external environment." RICCIO, E.L. e PETERS, M.R.S. *Ambiente virtual e flexibilidade: o impacto da tecnologia da informação sobre o sistema de informação contábil.* Revista de Contabilidade do CRC-SP. São Paulo: nº. 2, 07/1997. p. 6-7

the accounting controls will give them access and, through the accounting controls, they will hide their crime.

But, from another point of view, it is accounting, mainly under the form of system and computer auditing, that presents the best help for discovering these frauds practiced against companies' possessions. Accounting and mainly its professionals have to maintain themselves updated on the numerous "tricks" and "coups" that exist and intensify and adapt the internal controls to the new reality that appears.

There are many dangers. The defrauders are becoming bolder and bolder and have ever more modern and fast techniques at their disposal, which makes their crime faster, more overwhelming, safer and less detectable. Only knowledge can combat this kind of damage to organizations: ignorance and carelessness are some of the "enemy's" strongest arms.

7. REFERENCES

ATTIE, William. *Auditoria conceitos e aplicações*. 3. ed. São Paulo: Atlas, 2000.

CAMBRIDGE, *International Dictionary of English*. London: Cambridge Press, 1995.

CONSELHO FEDERAL DE CONTABILIDADE – *Normas Brasileiras de Contabilidade*. Da auditoria contábil. NBCT-11, 1999.

ELLIOTT, R.K. & JACOBSON, P. D. *Adding value to audits*. Camagazine, p. 35-7, 11/1997.

FERREIRA, Aurélio Buarque de Holanda. *Novo Aurélio século XXI: o dicionário da língua portuguesa*. 3. ed. Rio de Janeiro: Nova Fronteira, 1999.

GELBCKE, Ernesto Rubens *et all. Assurance Services: novas oportunidades para a profissão*. Boletim do Ibracon. São Paulo: nº. 248, p. 2-15, 01/1999.

KINDLEBERGER, Charles P. *Manias, pânico e crashes – um histórico das crises financeiras*. Tradução Vânia Conde, Viviane Castanho. Rio de Janeiro: Nova Fronteira, 2000.

KPMG (Stokes Kennedy Crowley). *Fraud awareness survey*. February, Rep. of Ireland, 1993.

LEVI, M. *Regulation fraud: white collar crime and the criminal process*. London: Travistock/Routledge, 1987.

MOSCOVE, S.A., SIMKIN, M. G., BAGRANOFF, N. A. *Accounting information systems: concepts and practice for effective decision making*. 4. ed. New York/USA: Wiley, 1990.

Core concepts of accounting information systems. 6 ed. New York/USA: Wiley, 1999

MOURA, Betina e HORTA, Ana Magdalena. *Uma terra de piratas*. Revista Época. São Paulo: Globo, year IV, nº 199, 11/03/02, p.84-89.

NEPOMUCENO, Valério. *O positivo e a neutralidade contábil*. Revista do Conselho Regional de Contabilidade do Rio Grande do Sul. Porto Alegre: nº. 105, p. 18-33, 08/2001.

NOGUEIRA, J. H. M. *A nova face do crime*. Revista de Perícia Federal. DF : nº 9, p.14-20.

PARENTE, F. A . F. *Auditoria de sistemas automatizados*. Fortaleza : Bco do Nordeste,1982.

PEAT MARWICK THORNE, *KPMTG international fraud survey report*. Toronto, 93/96.

RICCIO, E.L. e PETERS, M.R.S. *Ambiente virtual e flexibilidade: o impacto da tecnologia da informação sobre o sistema de informação contábil*. Revista de Contabilidade do CRC-SP. São Paulo: nº. 2, p. 5-11, 07/1997.

ROMNEY, Marshall B., STEINBART, Paul J., CUSHING, Barry E. *Accounting information systems*. 7. ed. USA: Addison-Wesley Publishing Co., 1997

SÁ, Antonio Lopes de. *Fraudes contábeis*. Rio de Janeiro: Tecnoprint, 1982.

Perícia Contábil. São Paulo: 2.ed., Atlas, 1996.

SOARES, A. P. *Sistemas eletrônicos de dados como fator preponderante na evolução da auditoria convencional*. Belo Horizonte: Unicentro Newton Paiva, 2000.

SOUZA, F. J. *A busca da evidenciação contábil em ambiente computadorizado*. Revista Perícia Federal. DF: nº. 3, p. 34-6, 10/1999a.

Perícia contábil e prevenção de fraude. Revista Perícia Federal. DF: nº. 1, p. 22-23, 03/1999.

A importância da avaliação do sistema de controle interno na perícia contábil. Revista Perícia Federal. DF: nº. 6, p. 12-13, 06/2000.