OBEGEF – Observatório de Economia e Gestão de Fraude

WORKING PAPERS

#12 How Portuguese small and medium companies deal with information security >>

Elisabete Maciel

OBEGEF
Observatório de Economia
e Gestão de Fraude

>> FICHA TÉCNICA

HOW PORTUGUESE SMALL AND MEDIUM COMPANIES DEAL WITH INFORMATION SECURITY

WORKING PAPERS Nº 12 / 2012
OBEGEF – Observatório de Economia e Gestão de Fraude

Autores: Elisabete Maciel[1]

Editor: Edições Húmus
1ª Edição: Novembro de 2012
ISBN: 978-989-8549-29-7

Localização web: *http://www.gestaodefraude.eu*
Preço: gratuito na edição electrónica, acesso por download.
Solicitação ao leitor: Transmita-nos a sua opinião sobre este trabalho.

Paper in the International Conference *Interdisciplinary Insights on Fraud and Corruption*

[1] Colaboradora do Observatório de Economia e Gestão de Fraude. E-mail: elisabet@fep.up.pt

>> ÍNDICE

>> **RESUMO**

No mundo empresarial contemporâneo as empresas manipulam e armazenam uma grande quantidade de informação, a qual é crucial para a sua sobrevivência. Tendo em conta o enorme impacto do avanço constante das tecnologias de informação, associado à obrigatoriedade da partilha de informação com todos os envolvidos no negócio (fornecedores, clientes, ...), as empresas não podem continuar a apresentar-se no mercado como "ilhas isoladas". Reconhecendo que informação é poder, torna-se um propósito essencial garantir a sua segurança. Existem várias normas (ISO / IEC 27002/Mehari) que definem as medidas a aplicar pelas empresas com o objetivo de implementar um sistema de segurança de informação. Contudo, muitas organizações não aplicam qualquer medida ou, se o fazem, limitam-se a adotar medidas inconsistentes, pouco frequentes e não estruturadas. Neste artigo, procuramos entender como as pequenas e médias empresas portuguesas lidam com este problema.

Palavras-chave: segurança da informação; requisitos de segurança da informação, ISO / IEC 27002; perceção do risco.

>> ABSTRACT

Companies store a large amount of information over the years that are crucial to survive in the contemporary business world. Taking into account the great development of communications, and the mandatory need of sharing information with their partners, organizations can´t work as "isolated islands" anymore. Assuming that information is power, it is therefore essential to ensure its safety. There are several frameworks (ISO/IEC 27002/Mehari) that define all the measures that organizations must apply in order to implement a security information system. Still, many organizations don´t apply any measure or if they do, they merely adopt inconsistent, infrequent and unstructured measures. In this paper we try to understand how Portuguese small and medium-sized companies deal with this problem.

Keywords*: Information security; Information security requirements; ISO/IEC 27002; Risk perception; Risk information*

>> INTRODUCTION

It is well known that companies are increasingly becoming more and more dependent of information systems. That situation is a consequence of a vertiginous development of information technology. The proliferation of personal portable computers, digital storing devices, mobile devices and all available mechanisms that allow sharing information on cloud, grants access, at any time and any place, to information required to run a business.

Most companies believe that their information systems are secure but the brutal reality is that they are not. However, companies information security concern is increasing in order to guarantee the information security. On the other hand, is not clear if the companies have a risk perception of the danger they incur by ignoring all the threats they are submitted daily.

Will a company be able to answer some basic questions concerning information security, such as:

- What are my security risk? What are my threats?
- What rules are imposed regarding the obligation of confidentiality relating to information and access to sensitive resources?
- Does the company promote human resources training about the security threats and the way to avoid them?
- Is the access to workstations and applications controlled against misuse?
- Is the information protected against internal/external attacks?
- What assurances can the company provide relating to information security requirements to their employees, suppliers, clients and partners?

Another relevant concern relates to the type of information a company manipulates. Some can deal with public information and/or private information like customer portfolio, strategic decisions, etc. On the other hand, some companies deal with internal and sensitive information to others like health or fiscal information of their clients and what may have legal obligations associated.

To deal with information security is necessary to implement control measures. The ISO/IEC 27002 framework is a code of practice for Information Security Management accepted as an universal guide to achieve that purpose (Calder and Watkins, 2008). It presents eleven security control clauses (security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition,

development and maintenance, information security incident management, business continuity management and compliance). Our approach will only focus the security policy, the human resources, the communications and operations management, the access control and the information security incident management.

The Portuguese business structure is based in micro, small and medium size companies. According to National Statistical Institute (INE) in 2009 there were 1 060 906 non-financial companies and 99,92% (1 060 018) of them have less than 250 employees - micro, small and medium. 4,33% (45 915) of these companies are small and medium-sized companies (SMEs). However, SMEs represent 63,91% of all the turnover of micro, small and medium companies and 44,96% of all the employees. SMEs will be the target of this study.

Our option of excluding micro companies is supported on the relation between size and turnover. If the available resources of a SME capacity to invest in information security are limited, then that investment is overwhelming for micro companies.

Our goal is to describe if the SMEs surveyed have the minimum requirements and satisfactory management of information security, using as reference the controls presented in the information security standard ISO/IEC 27002.

It's important to know how the SMEs in Portugal deal with this reality. With the vertiginous development of information technology the threats grows exponentially: wireless networks, portable storage equipment, outsourcing of equipment (server, storage), software and services, cloud computing and so on. Until now, there isn´t any systematic study of this kind in Portugal.

>> LITERATURE REVIEW

Our first concern is to clarify what ISO/IEC 27002 understands by "information security".

First of all, we must attend to its definition of information: "Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected".

Citing the international standard, "Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities."

To do so, "Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met."

The Internet massification, the decrease of computer prices and the increasing requirements to conduct business using electronic means are forcing companies of any size to rely on technology to manage, store and transmit vital information. The situation is even worse when referring to small companies that, due to its limited budget, are obliged to outsource resources and services, with all implications this involves. This situation is appealing to those who think, that they may have something to gain from damaging or stealing this valuable information: hackers, crackers, unsatisfied employees, competitors, a cyber thief.

Companies are more and more dependent on information systems in order to take advantage over their competitors. Kankanhalli et al. (2003) concludes that small and medium enterprises invest less in information security than larger organizations. So, SMEs are more vulnerable to information attacks.

According to the sixth Global Economic Crime Survey (2011) dedicated to cybercrime and elaborated by PricewaterhouseCoopers (PWC), cybercrime is defined as "an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."

With the participation of about four thousand organizations in 78 countries[1], this last survey concludes that cybercrime is a growing threat. Some conclusions are disturbing: 34% of respondents experienced economic crime in the last year; 56% said the most serious fraud was an 'inside job'; 42% had not received any cyber security training.

Other conclusions are presented by the Information Security Breaches Survey carried out by PWC at 2010. The value of this survey is the differentiating results between large (more then 250 employees) and small companies (less than 50 employees), but only in the United Kingdom. It is noted that 34% of the companies are critically dependent on externally software services over the internet. The most common externally hosted services are websites (46%) and email services (27%), but nearly a quarter uses third parties for payment and payroll processing. We would like to highlight some relevant conclusions relating to small business: 67% have documented information security policy; 85% use a wireless network; 47% use Voice over IP (VoIP); 63% allow staff remote access to systems; 83% had a security incident in the last year (58% were reported as accidental and 74% as malicious); 42% were staff related incidents (most of them due to staff misuse of web and email).

The Global Information Security Survey has been carried out for fourteen years by Ernest & Young. The 2011 survey was submitted in 52 countries and was answered by 1700 organizations. The findings important to this paper are the following: only 52% of respondents have a documented security strategy; only 20% of respondents do not have plans to permit the use of tablet computers; 36% of respondents use cloud computing; 53% of respondents have implemented limited or no access to social networks as a way to control or to mitigate risks related with it.

Gupta and Hammond (2005) share the opinion that the academic investigation carried out relating to information security of small organizations (adopted criteria - between 10 and 499 employees) is insignificant. They found that covering 138 United States small companies, these are less likely to have a documented information security policy. Besides that, they have very low security breaches (19%) and they view virus attacks as a top five security concern.

A study that took place in Brasil (Netto and Silveira, 2007), concerning 43 SMEs metal manufacturing industries, concluded that the companies main investment is in technology, in order to decrease the security incidents, forgetting the human factor, which is frequently the principal cause for security

[1] Portugal is one of the few European countries that has no representation at this survey, although there was one respondent at the 2009 survey.

breaches. The companies use the antivirus as the main security tool. In that paper the authors had selected only 20 controls of the 127 present at ISO/IEC 27002 standard and were expecting a good adjustment from the survey results. However, they verified an inadequate adaptation which can be the result of lack of time and/or money. We can't forget that the sample is composed by small size companies.

>> METHODOLOGY

To perform this analysis we decide to implement a survey built by us and supported by international standards. A web survey presents some advantages: a smaller transmitting time, a lower delivery cost, much more design options and a shorter data entry time (Fan, 2009 and Solomon, 2001). This goal was achieved by sending invitations (by email) to companies so they could easily respond to the web survey. We are aware that this type of survey presents some limitations. Some of the most visible are the requirement of an internet access, an available email and a low response rate. (Fan, 2009).

The first step is the definition of our population. Our source was the database SABI (Sistema de Análise de Balanços Ibéricos) a financial information and business intelligence for companies in Spain and Portugal in 2010. There we found 47 855 SMEs (between 10 and 249 employees). Taking into account that in the north of Portugal we find the biggest concentration of SME, we decided to confine our focus to Oporto district (21% of the SMEs). The next step was the selection of activity sectors. We decided to choose those sectors in which the information is crucial for its business. Finally, to do a web survey we could only choose those from whom it was possible to send an email. Our population is composed by 1531 SMEs from Oporto district of some sectors (see table 1) with email address.

Referring to the sectors, we can see at table 1 there is fair representation of companies when we comparing our population with all Portugal SMEs.

We found that the medium companies are over- represented in our population (table 2).

Consulting the literature, we developed our survey in terms to counteract the factors that normally affect the response rate: not very long (30 questions); only with closed questions; objective; simple design; contact via a personalized invitation; no attachments; providing contact information for needed help; guarantee of an easy and secure access (use of token); use of reminders.

This survey was implemented using the LimeSurvey platform and the first invitation was sent on the 30th of May of 2012 to all 1531 SMEs. After that, we sent a weekly reminder for three weeks and received a total of 152 valid answers (9,9%).

Table 1 – SMEs companies by sector: Portugal versus population

Sectors	Portugal		Population	
	Number	**Percent**	**Number**	**Percent**
Manufacturing	13.829	44,1%	674	44,0%
Electricity, gas, steam and air conditioning supply	50	0,2%	3	0,2%
Water supply; sewerage, waste management and remediation activities	255	0,8%	24	1,6%
Wholesale and retail trade	10.568	33,7%	567	37,0%
Information and Communication	869	2,8%	56	3,7%
Financial and insurance activities	254	0,8%	14	0,9%
Real estate activities	478	1,5%	5	0,3%
Professional, scientific and technical activities	2.043	6,5%	100	6,5%
Administrative and support service activities	1.771	5,6%	59	3,9%
Human health and social work activities	1.273	4,1%	29	1,9%
Total	**31.390**		**1.531**	

Table 2 - SMEs companies by size: Portugal versus population

Number of employees	Portugal		Population	
	Number	**Percent**	**Number**	**Percent**
Between 10 and 49	41779	87,3%	1154	75,4%
Between 50 and 249	6076	12,7%	377	24,6%

We verified that only 62 (4%) companies rejected the sent emails (invitation and reminders). 28 of them rejected the messages due to mechanisms of security control (message appears to be unsolicited). The others presented justifications as: user unknown, mailbox is full, etc.

Taking in account that our goal was to probe SMEs sensibility to information security, we tried to assure that the respondent had some kind of leadership role because we believed he/her could have some involvement concerning the management of information security.

We concluded that 83% of the respondents (figure 1) of our sample had a leading position at the company.

In addition to the basic questions, in order to characterize a company: geographic location, number of employees using or not computers, number of computers (with or without internet access), type of information that is manipulated, all others questions were produced using as reference the framework ISO/IEC 27002. Table 3 gives a brief description of the issues addressed in our survey.

Figure 1 - What's your role at the entreprise?

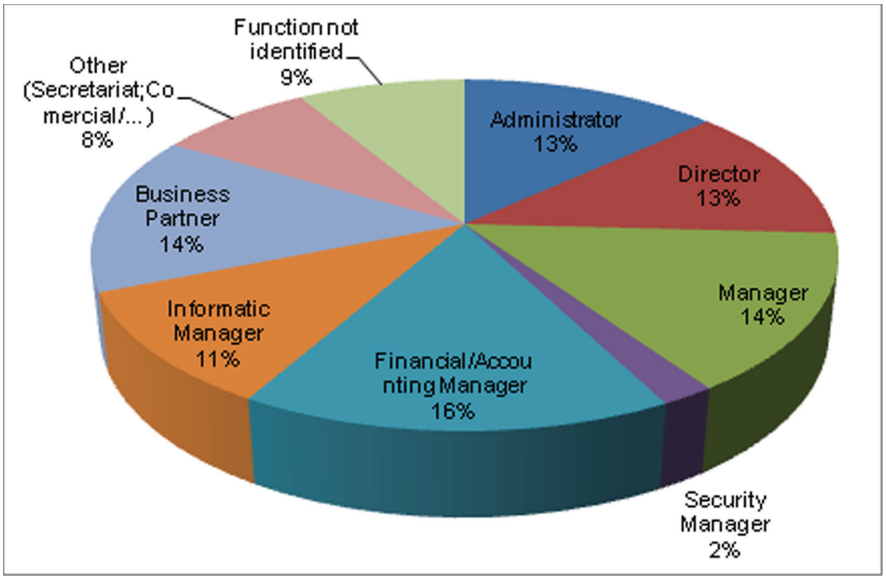


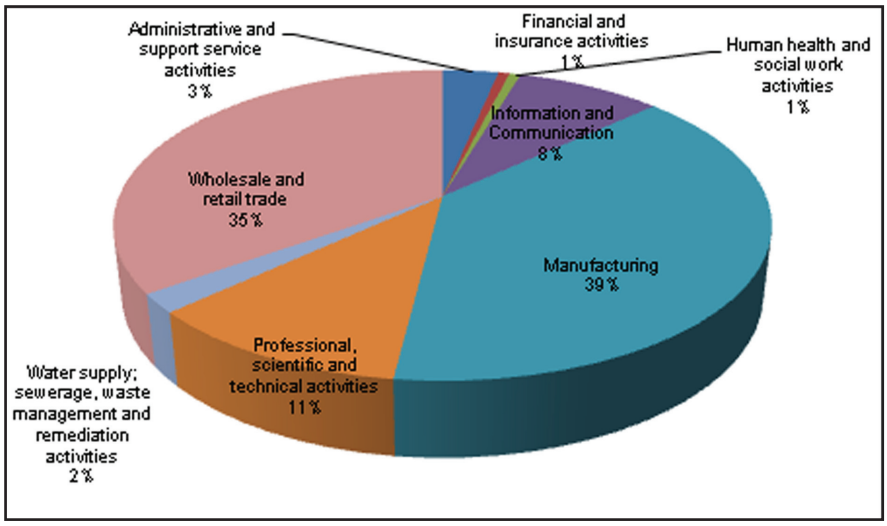
Table 3 – Web survey

Security Control Clause	**What to investigate?**
Security Police	(a) Whether there is an information security policy and if it is reviewed frequently.
Human Resources Security	(a) Whether the company guarantees, in a contractual manner, the confidentiality of sensitive data with the one(s) that deal with it; (b) Whether is verified, as a prior employment condition, the security roles and responsibilities to be assumed; (c) Whether the employees receive appropriate security awareness training.
Communications and Operations Management	(a) Whether exist detection, prevention and protection against malicious and mobile code; (b) Whether regular backups of information and software are done.
Access Control	(a) Whether there is a formal registration for granting access to all information systems and services; (b) Whether the use of any privileges in information system environment is restricted and controlled; (c) Whether there is a network connection control, especially, in respect to the internet; (d) What kind of technologies are used (wireless, Bluetooth, remote access, VoIP, cloud computing, ..); (e) Whether a policy is in place, in order to guarantee the protection against the risk of using mobile computing.
Information Security Incident Management	Whether any security incident (virus attack, DoS, fraud, ...) took place and what is its origin.

>> RESULTS

First of all we are going to characterize the 152 companies that are part of our sample. We verified that 118 (77,6%) are small and 34 (22,4%) medium companies. Manufacturing and wholesale are the most representative sectors (74%) – see figure 2.

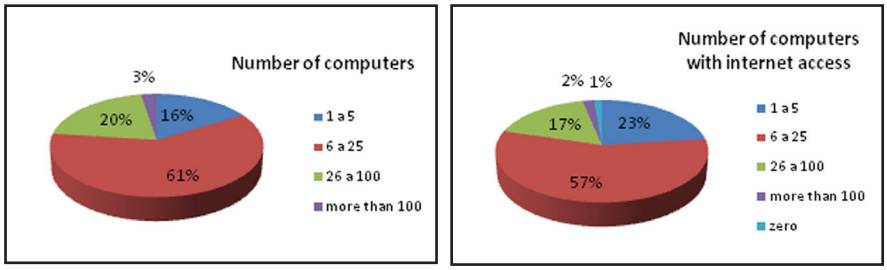
Figure 2 - Companies by sector



Only 3 companies from the manufacturing sector have no server. On the other hand, 78 (52%) of the sample have 2 or more servers. Figure 3 shows how companies are equipped, regarding personal computers/workstations with or without internet access. As expected, the number of computers/ workstation with internet access is very significant.

As we can see, most of the companies have internet access, which represents an added risk to their security information. About 80% of the companies use wireless and 62% allows remote access. 25% uses voice over IP (VoIP) and in a more incipient way 12% use cloud computing. The medium companies

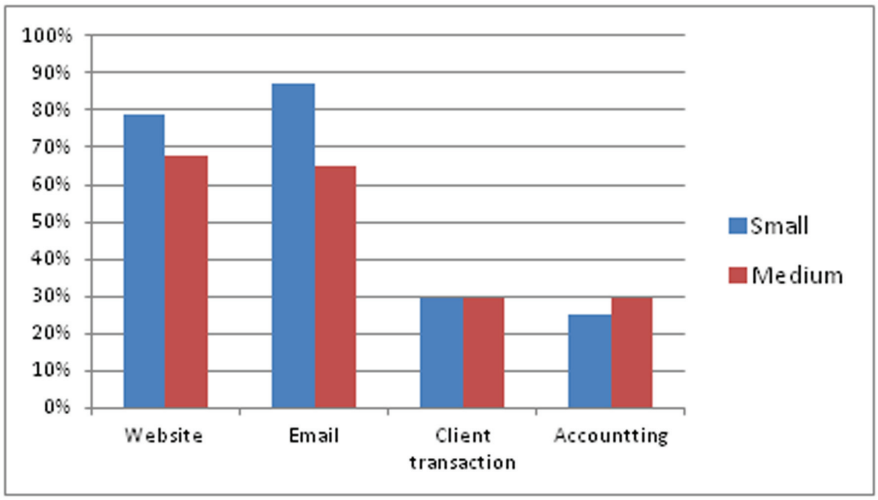
Figure 3 – Companies by number of computers/workstations



are the ones that make more use of VoIP and cloud computing when comparing with small ones: VoIP (32,4% vs 23,7%) and cloud computing (17,7% vs 10,2%). However, this difference is not statistically significant.

On the other hand, we verified that outsourcing of services is very common, essentially those who are supported in network communications - mostly email. Figure 4 shows that many companies outsource services for website and email. Small companies are much more dependent on email outsourcing (64,7% vs 87,3%). This difference is statistically significant (p=0,002).

Figure 4 – Outsourcing services



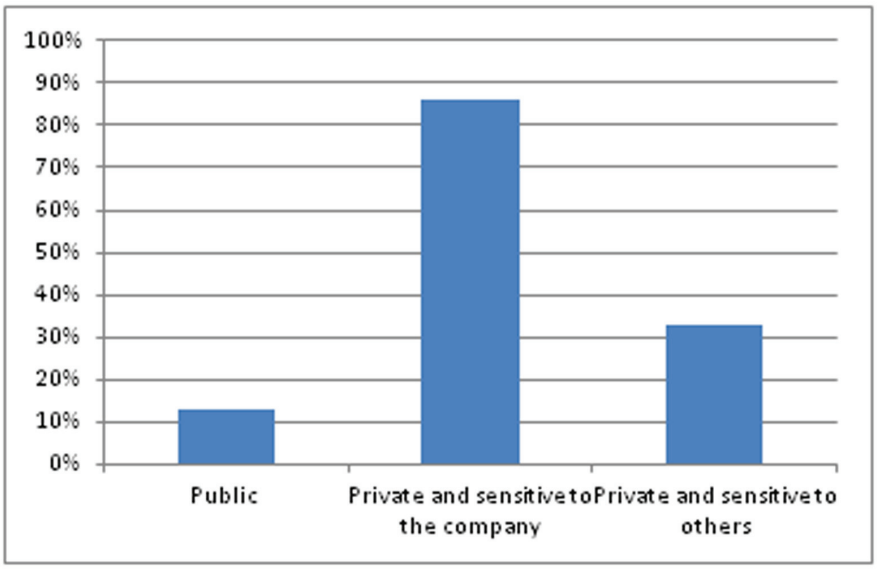
Another source of problems that contributes to risk security is a gap that may result from the permission to connect private equipment (pen, tablets, and so on) of employees to the company network.

From the survey we verified that about a quarter of the companies allows any employee to connect any device with no restrictions or limitations. About 45% companies don't allow any connection and only 27,6% allows access but with very clearly defined rules. The way, medium and small companies, deals with this problem don't differ much in the case where the connection is forbidden (medium – 44,1% and small – 45,8%). However, the situation is quite different when a company allows connections without any rules (medium – 29,4% and small – 22%) or defines strict rules to allow a device connection (medium – 17,6% and small – 30,5%). Probably this may be a consequence of a medium company, by having more technological resources available and an IT Department, think it is better protected against attacks.

Another interesting analysis has to do with the type of information that is handled by companies. According to figure 5, we believe that companies deal,

mostly, with sensitive information for running its business. Apparently, this situation is independent of company size. However, we concluded that, according to company sector, there is a significant statistically difference related with the type of information.

Figure 5 - Type of information manipulated



The results of the survey regarding the *Security Policy* of the ISO/IEC 27002 control clause reveal that 47,9% of the 144 companies that assumes they are aware of its situation, have documented rules/procedures in order to guarantee the information security. 38,2% said that there are rules, but are not documented, and 13,9% have no rules at all. Although not statistically significant, there are some differences according to company size: rules documented (medium – 60,6% and small – 44,1%) and not documented (medium – 27,3% and small – 41,4%). It's important to highlight that about 30% of the companies that have defined rules, don't update them on a regular basis.

With respect to *Human Resources Security* we verified that, although most companies deal with sensitive information, only 42,1% have defined rules about confidentially obligation when it comes to their employees and 13,8% don't define any rules at all. On the other hand, only 36% of the companies that have defined rules for information access, guarantee them in a contract signed by the parties. We found no statistical evidence that the existence or not of rules has any relation to the size/sector of a company.

Another interesting finding relates to the companies concern with the employee training in information security threats and how to prevent it. We

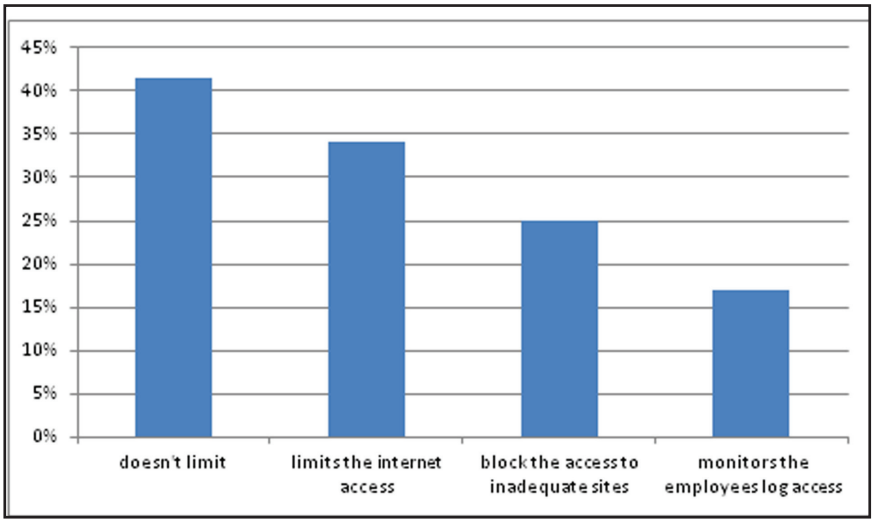
found that 40,8% don't give any training. Only 14,5% gives training in a regular base. The rest of them gives some occasional training. Although not statistically significant, we can observe that the medium companies that don't give any training are more than the small ones (medium – 52,9% and small – 37,3%). On the contrary, the small companies gives more training to its employees.

Another important subject as to do with the examination of the professional/civil information of a new employee before he can deal with company information. We verified that almost 40% of the companies don't analyze the professional/civil information of a new employee. 30% of the companies only do it if an employee is going to work with sensitive data.

Another two ISO/IEC 27002 controls as to do with *Communications and Operations Management and Access Control*. Most of the surveyed companies protect the access to computers/workstations and to applications using password. Only a few cases are in open access. Regarding to information access, almost 75% of the companies have restrictions according to employee profile. However, there are 11,2% of the companies where any employee can reach any information. Most of the companies in this situation, are from manufacturing, wholesale and retail trade and administrative and support service activities sectors.

It is important to know how the companies control the employee's abuse on the access of web sites and social networks. Attending figure 6 we perceive that more than 40% of the companies doesn't limit the access.

Figure 6 - Control access to web sites



We verified that the medium companies are most effective when we talk in the action of blocking inadequate sites: 35,3% for the medium companies and 22% for the small ones. The situation is the same when we talk about monitoring the employee logs where we find a significant difference (p=0,001). 35,3% medium companies monitors the employee logs against 11,9% small companies. Once again, this situation as to do with the, probably, existence of an IT Department.

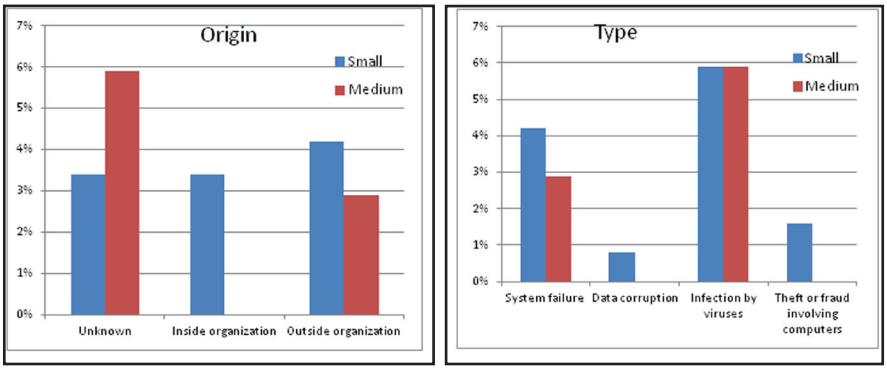
As we state previously, most of the companies have internet access. However, we still found four small companies (three of them from the manufacturing sector) without an antivirus.

Another basic operation that is responsible for avowing information loss is the backup. Almost all companies in the survey do regular backups of theirs servers. We verified that about 7% of the companies outsource this process: more the small ones (about 8%) than the medium size ones (about 6%). Against our expectation, we found a medium size company that doesn't do any backup of the server. When refer to the computers/workstations, we noted that about 25% of them let this backup responsibility to the user. In this case, we verified that 3,3% of the companies (all small) outsource this task.

About the *Information Security Incident Management* we found that only 10,5% of the companies reported some kind of incidents in the last year: 11% were referred by small size companies and 8,8% by medium ones.

The companies report that the origin of the incidents are mostly unknown or caused from outside of the organization. Strangely, medium companies have no incidents induced inside the organization (see figure 7).

Figure 7 - Origin and type of incidents



The most common incident referred originates from virus infection, not distinguishing small and medium companies. However, we found that the manufacturing and wholesale sectors are the most affected.

>> DISCUSSION AND CONCLUSION

This study intends to obtain a characterization of small and medium size portuguese companies, with reference to ISO/IEC 27002 standard in order to evaluate if those companies are sensitive to several mechanisms that may contribute to prevent fraud.

One of the security control clause that is systematically depreciated refers to human resources. Our study corroborates this conclusion: generally, the contract of a new employee that will have access to company information, is not preceded by an inquiry to his/her previous professional/personal life; in most cases, there is no employee/supplier/client/partner obligation of confidentially when concerning the manipulation of sensitive data; furthermore, companies neglect the essential mandatory training of theirs employees in order to prevent information security threats.

It is preoccupying the absence of rules to manage the connection of external devices (mobile phones, external storage, PDAs, tablets, portable computers, etc) by employees. There is a general consensus that this is an additional focus to risk information. This situation becomes even more serious when it is assumed by 86% of the companies, that the information manipulated is private and sensitive for running the business. Another concern is the fact that many of the companies do not limit internet access to their employees. This will certainly increase the risk of information security.

Another interesting conclusion refers to the different behaviour of small and medium companies with respect to this thematic. Although not proven, it is expected that a medium-sized company has an IT department that contributes to avoid the basics risks of communication and operation management. An important clause that reports the need of documented rules in order to guarantee information security is best fulfilled by medium size companies. When we talk about services, small companies use more frequently outsourcing, which implies more vulnerability. On the other hand, small companies are more reluctant to adopt new technologies: VoIP, cloud computing. It is not clear if that option is a consequence of having no idea of the risks that may occur when it comes to information security or if it is only reluctance to change.

Based on international studies, it is doubtful that the number of reported incidents on this survey correspond to reality. Besides, incidents origin is announced has being outside the company (or unknown) and majority by virus infection. Only one company was subjected to a theft or fraud involving

computers and another one indicates that its security breach was originated in passing sensitive information to competitor. In futures studies, these questionable results must be investigated.

In future studies it will be interesting to inquire for the existence of information security expenditure properly itemized: technology and human resources. Another point of investigation could be a potential measure of risk perception. Moreover, it will be significant to investigate an eventual application of ISO/IEC 27002 standard (or a simplified version), in order to carry out an efficient formal security policy.

It will be interesting to extend this study to a large-scale (e.g. national sample for all sectors) and to do it periodically in order to observe the behaviour alterations in companies practice: security policies, procedures adopted and technologies implemented.

We mustn't neglect the effect of an inexistent policy of information security may have to a company and, in a global perspective, to a region or a country. A well implemented security policy supported in the standards may avoid serious incidents (out of service, theft, fraud) which have real costs to the company/country. We must recognize that every day the threats are even more sophisticated and the global network it's a facilitator.

References

Calder A. and Watkins, S., 2008. *IT governance : a manager's guide to data security and ISO/IEC 27001/ ISO/IEC 27002*. 4rd ed. London and Philadelphia: Kogan Page Limited.

Empresas em Portugal 2009, INE, 2011

Fan, W, and Yan, Z., 2010. Factors affecting response rates of the web survey: a systematic review. *Computer in Human Behavior*, 26(2), 132-139.

Gupta, A. and Hammond, R., 2005. *Information systems security issues decisions for small business: an empirical examination. Information management & Computer Security*, 13(4), 297-310.

International Standards Office, 2005. ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security management. Geneva.

Kankanhalli, A., Teo, H., Tan, B. and Wei, K. ,2003. An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139-154.

Netto, A. and Silveira, M., 2007. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e mádias empresas. *Revista de Gestão da Tecnologia e Sistemas de Informação*, 4(3), 375-397.

Solomon, D., 2001. Conducting Web-Based Surveys. *Practical Assessment, Research & Evaluation*, 7(19).