Security policies for small and medium enterprises

A.Kanellos, V.Dimopoulos and N.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

Over the last few years, the advances in information technology have brought many changes to the business environment. More and more businesses now try to take advantage of the technologies and applications that promise to help them improve many of their tasks. Companies of whatever the size are now becoming increasingly reliant on the Internet to fulfill many of their basic functions and ultimately to remain competitive in the demanding marketplace. Many of them are now conducting transactions over the Internet using email and other applications to make some of their tasks more efficiently and to improve their relationship with their customers. But as they increase the level of their connectivity to the Internet and the applications surrounded by the web, they increase the potential of a malicious security breach that could harm the business continuity and that could result ultimately in significant losses. Hence some sort of protection measures are now considered necessary for businesses of any size with the security policies regarded as the first and most important of them. Controversially to that aspect small and medium enterprises are found through major surveys like the DTI and the CSI/FBI security surveys to lack sufficient protection since the majority of them reported not to adopt or having difficulties to adopt security policy practices. In general, the findings from various surveys are quite discouraging for the small and medium firms as far as security protection is concerned. Because of this situation some sort of solution was investigated and provided by this paper by taking into consideration the factors that minimise the adoption of security policies in the SMEs. In addition, the solution described takes into account the potential of using baseline guideline documents.

Keywords

SMEs, information security policies, information security

1. Introduction

In the recent past, a number of surveys were conducted worldwide on the security issues taking into investigation businesses of any size and subject. Such surveys that were conducted by well known authorities like the DTI Survey 2004 from the Department of Trade & Industry in the UK and the CSI/FBI Computer Crime and Security Survey 2004 Computer Security Institute in the United States indicated the behaviour of SMEs towards the use of security policy practices.

The surveys indicated that the information security is related to the size of the company and, being more specific, the level of approach to security practices (like the use of security policies) shown by a company decreases as the size decreases. Small and medium sized companies are found to be missing security practices and most importantly security policy documents. There exist, though, some factors that

hinder the small and medium enterprises from adopting adequate security practices. These factors as well as others were investigated in order to identify the specific needs of the small and medium sized companies towards security procedures and to provide consequently proper solutions for them. This paper presents an investigation into the lack of security practices in SMEs identifying the reasons for the minimised adoption of security policies and proposing some solutions that aim to improve the security practices within a SME organisation.

2. Security survey findings

As a start point in this paper the findings around the security practices in small and medium companies are going to be presented. The findings below that were collected from major security surveys illustrate the security behaviour in small and medium sized businesses and, as a result, in what extend they adopted security measures and especially security policies. The surveys were conducted on the businesses of any size but since the majority of them were small and medium businesses we can state that their results can give us a clear idea about them. The surveys that were used were the following:

- DTI Survey 2004 - Information security breaches survey 2004 technical report
- CSI/FBI - Computer Crime and Security Survey 2004
- Ernst and Young - Global Information Security Survey 2004
- Deloitte Touche Tohmatsu Org. - 2004 Global Security Survey
- 2005 Australian Computer Crime and Security Survey
- 2002 Information Security Magazine Survey – Does size matter?
- E21-MagicMedia - E-security survey report

A major finding from the above surveys was that the majority of small and medium enterprises lack documented security policy practices. Only the 39 percent of the small and medium enterprises adopt a security policy according to the E-security survey report. In addition to the effect on the use of security policy, the size of the organisations was found to be also important in the security awareness of the organisation. More specifically, we can say that the larger the organisation, the more mature its security awareness. (Melek, 2004)

Moreover, outsourcing of security functions seems to be a more common finding in larger organisations rather than in the smaller ones. Only a very small percentage of the small and medium sized enterprises considered outsourcing of security functions with the lack of budget reported as their great obstacle. Figure 1 below illustrates the percentage of respondents according to the level of outsourced functions.

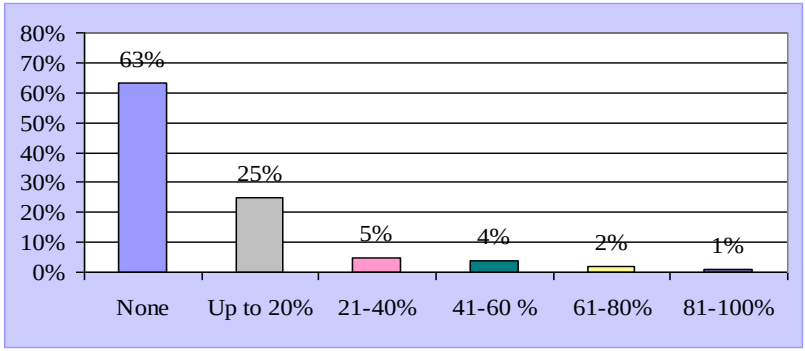

Figure 1: Security functions outsourced by businesses

Source: CSI/FBI - Computer Crime and Security Survey 2004

It can be easily derived that only a small percentage (25%) of respondents, and in fact SMEs, outsourced a respectable portion (up to 20%) of their security practices while the majority of them outsourced a very small percentage or no percentage at all of their security practices.

Another finding is that SMEs spend only a small portion of their IT budget on security. Most of the SMEs tend to spend a small percentage of their budget on security either because they have restricted budgets in general or because they do not feel that security is an important issue. So the amount spent on IT security is not adequate enough to support the security practices and provide an acceptable level of robust security (S. Timms *et al*. 2004). Figure 2 below gives a notion of the money spent on security.

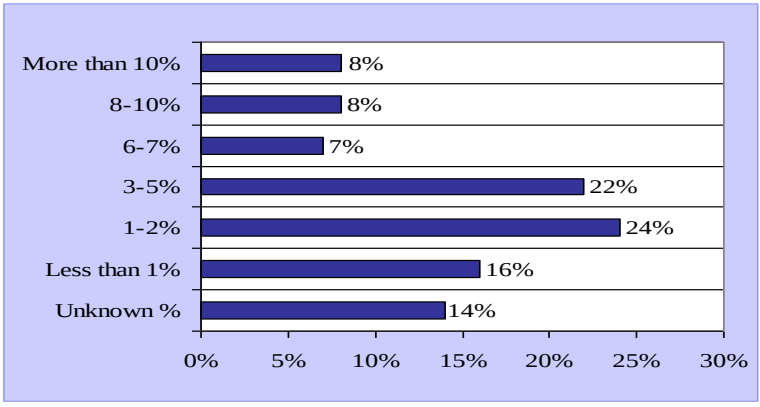

Figure 2: IT budget spent on security

Source: CSI/FBI - Computer Crime and Security Survey 2004

The more disappointing fact is that in addition to spending a small percentage of their annual budget on IT security, they also often feel that their organisations are adequately protected. And in addition to their minor investments on security and the poor security measures, they feel that they are adequate protected. Because of that

many of the enterprises failed to conduct a regular assessment and re-evaluation of their security policy even if an 82% of the organisations conduct some kind of security audits that could be very useful for something like this. (Gordon *et al*. 2004)

In addition to the above, the education and training process was found to be poor in many organisations despite that it is perceived valuable in many of the aspects of security like the network security, the security management, the economic aspects of computer security, the security systems architecture, the investigations and legal issues, the cryptography, etc. (Gordon *et al*. 2004) It is described that about 70 percent of the respondent companies failed to list employee training/ education as their important priority in the IT budget. (Ernst and Young)

The risk management process that is the main part in the process of creating a security policy and hence protecting the company's assets was also found to be missing in most of the enterprises and hence SMEs (Melek, 2004). There is even a percentage of them that failed to complete successfully the risk management process due to mistakes in the process. Because the small and medium enterprises in general lack personnel with sufficient expertise they are not able to recognise the assets and their importance as a first step and the security breaches that may consider a potential risk as a next step. On the contrary, 89 percent of the enterprises feel that having a risk management process within the organisation was either extremely or very important. (Melek, 2004)

3. Reasons for the minimised adoption

In the previous section we have identified through surveys that small and medium enterprises lack sufficient security protection due to the lack of security policies and we also described some reasons for this minimised adoption. In this section we are going to give a better description of these factors and provide some other too.

3.1 Lack of security policy guidelines for SMEs

The lack of security policies guidelines for SMEs can be attributed to two separate factors. First of all it is the fact that it is difficult for someone to find security policy guidelines that are written especially for SMEs and secondly it is the fact that even if they find some papers that claim to provide guidance for the SMEs these papers are not covering all the aspects of security. Most of the security white papers and any baseline guideline documents are mainly written with a general subject so that any size of business is supported. Moreover, by going through some of them it can be realised that they are more appropriate for use by security specialists with a good knowledge background on security. In addition to the difficulties in finding security policy documents for the SMEs, the few of them available contain a number of flaws. Having a look at papers that claim to provide guidelines for the security practices of the SMEs we can realise that these papers basically provide a detailed tutorial on implementing hardware and software security with other important aspects of security missing like the risk management and education process.

3.2 Budget limitation

One of the greatest hindering factors towards adopting security practices in the SMEs is the lack of sufficient budget allocated on security. It is indicated that smaller organisations are spending less on security than the larger ones while they spend a greater percentage of their IT budget on security as shown in Figure 3 below. This can become reasonable if we take into consideration the fact that the amount of security budget becomes smaller as the size of the company decreases. An average security budget for a small enterprise is $132,000 per year, $360,000 for a medium one, while for a large enterprise reaches the $1.3 million per year.

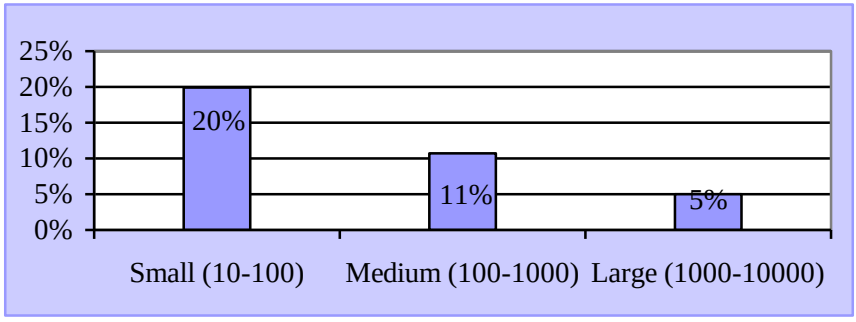

Figure 3: Percentage of IT spending on security according to business size
(source: Briney and Prince, 2002)

3.3 Lack of security specialists

Many businesses are too small to be able to justify in-house security specialists. According to the DTI survey 2004 three-quarters of UK businesses obtain external advice on security matters and only the 42 percent of them have somebody with IT qualifications. In some cases it is not only the fact that the enterprises cannot justify in-house security specialists, but moreover it is the security personnel that they feel that the environment in a small business is not what they are looking for. For whatever the reason, the fact is that small and medium enterprises are equipped with personnel that lack or do not have the adequate security qualifications.

3.4 Lack of incentive

It was found from observations and interviews that organisations may not adopt security procedures without the appropriate incentive. The senior management has to be convinced, in other words, that reducing risk by improving information security is worth the investment. And this is a difficult issue if we consider that the value of information security countermeasures is not visible since it is based on disastrous events. Making matters worse, there is no well-understood economic model for evaluating the benefits of using security procedures and policies as a mean of reducing threats. (Ernst and Young 2004, Timms *et al*. 2004)

3.5 Others

In addition to the above there are other less important reasons that may hinder the adoption of security policies in small and medium enterprises. Firstly, the pace of information technology changes acts as a hindering factor which makes matters worse for small and medium enterprises that already suffer from insufficient security budgets. The complexity of some provided solutions when considering the hardware and software can add difficulties when identifying the suitable measures for establishing the appropriate security policy. Finally, it is simply the case that the security policy procedures are being put aside for 'more important things' that acts as a preventive factor. (Ernst and Young 2004, Internet Industry Association 2003, Dimopoulos *et al*. 2004)

4. Proposed solutions

Now that we have identified some of the basic issues around the lack of security policies in SMEs it is important to introduce some sort of solutions so that the small and medium companies can adopt more widely security practices. In order to rectify this situation initially the limiting factors that are found in SMEs must be considered and then some sort of specific guidance in accordance with the use of baseline guideline documents must be provided. The paper we will simply try to present a simplified procedure for creating a security policy.

4.1 A simplified procedure for security policy

As a starting point the IT management can simply separate individuals into categories according to their needs and the level of access needed to the company's information system. For example, the following groups can be specified: users, administrators, guests, third parties that cooperate with the company, customers, etc. By doing this the obligations and tasks for each group can be dealt separately.

The next and most important step is the risk management process. According to this proposed solution the company's assets, that need to be protected and that may be targeted by a security threat, are initially identified and imported in a list. As asset we can define anything that needs protection including databases, information, personnel, facilities, applications, computer hardware and software, and communications systems. After that, it is time to identify the possible security threats that are associated with the assets and that may target them such as earthquakes, viruses, hackers, data destruction/ modification/ theft, theft of company property, fire, sabotage, fraud, or embezzlement. From information security surveys or other similar sources that can be found easily and free at the Internet (e.g. CSI/FBI – Computer Crime and Security Survey) the importance of the security threats can be also defined. A list that contains all the possible security threats sorted according to their importance must be produced at this point. Going forward it is now necessary to estimate the impact of the identified threats to the company's assets. Towards this some sort of statement phrases should be produced like in the list below. Together with each statement phrase the importance of the impact must also be added. The importance must be estimated according to the consequent losses for the enterprise

such as financial losses, business continuity disruption, incident response costs, data loss and disruption. (HKCERT Coordination Centre, Hamilton) The list should be sorted according to the importance field so that it looks like the following example:

Impact of security threats to business	Importance of impact
E-commerce server down due to DoS attack	9
Reveal of business data to competitors due to theft	7
Loss of business continuity because of attack on the company's network	5

Table 1: Example of list with statement phrases

Having done the above, we can proceed to produce any possible countermeasures. In order to define the possible countermeasures the security administration must first examine carefully the last two lists mentioned previously in order to realise which of the risks are worth considering and which not. An 'impact of security threat to business' that is highly rated, while the threat is also highly rated, introduces a risk of high importance that requires countermeasures to be introduced. As countermeasures we can define any of the security controls that can be employed to eliminate, reduce or mitigate the impact of a threat occurrence. The table above, for example, that shows that a DoS attack on the e-commerce server can cause significant losses and hence is of high importance indicates that intrusion detection software and firewall must be established. It is assumed that it has already been found that DoS attacks are frequent and hence regarded as important. (HKCERT Coordination Centre, Hamilton)

As a last step in the risk management process the senior management of the organisation must select which of the countermeasures will be implemented in the company's information system. The selection is based on cost issues and uses the ROI (Return Of Investment) analysis that is easily comprehensible by the organisation's senior management. According to this the benefits of the proposed security countermeasures specified by the security administration team are all introduced to the senior management in term of their investment and the return of investment costs. (Cisco Systems, Inc. 2004) In other words, for each of the countermeasures the cost for establishment (investment) and an estimation of the money saved on a long term basis (return of investment) are required. The senior management of the organisation can then decide according to the aforementioned costs which of the proposed security countermeasures are worth applying to the organisation and which not.

Once the countermeasures have been defined the next step is the security policy creation. The construction of the security policy document, which will specify what is acceptable and what not for everyone working inside the business environment, can be simplified by breaking down security into individual segments and dealing with each of them independently. Having the notion that security should be limited only to the absolutely necessary can also help in the simplification of the process. The responsible for the construction of the security policy should not worry about producing a well articulated security policy with their first attempt but must go

through the review and evaluation of the policy and possibly the construction of a new policy document.

5. Using ISO/IEC 17799

Towards increasing the security awareness and improving security practices in small and medium enterprises there is also the potential of using baseline guideline documents. The ISO/IEC 17799 document is one of them providing an extensive guidance on organisational aspects of information security management. The ISO 17799 code of practice can be a good starting point for the small and medium enterprises to implement information security. It can help the inexperienced personnel of the SMEs to identify the areas of the information security that need to be considered. Having identified the areas that need attention, the IT personnel will simply have to follow the recommendations on the corresponding sections. In addition, baseline guideline documents like the ISO code of practice or the NIST handbook are provided by organisations and institutions that may have a dominant position on national or international scale and their quality definitely reflect the expertise in security of the organisations they belong to.

In the small and medium enterprises, though, the ISO code of practice cannot be easily adopted and used widely by their personnel that may lack knowledge and experience on security issues. That is because the ISO as well as other baseline guideline documents just provide the framework for introducing security practices without going in depth to give details of specific countermeasures to follow. Hence we can say that the ISO is more appealing to security experts that can take the information provided by the document and implement security solutions according to the needs of the organisation.

As a way to help the small and medium enterprises in using more widely the ISO code of practice, the document must be initially minimised so that to include only the aspects that are necessary for the SMEs. Some of the sections provided in the ISO 17799 can be regarded as optional and can put aside for other more important. For example the sections “information classification” and “security in job definition and resourcing” are some of the sections that can be regarded as optional. Going further the ISO code of practice can be enriched with more details in each of its sections so that is more comprehensible by the personnel of the SMEs that may lack sufficient knowledge and experience on security. Detailed steps for the proposed security solutions together with explanations of information security terms (e.g. what we define as asset, security policy, threat, etc.) is the extra information needed so that the ISO code of practice can become more appealing for the personnel of the small firms.

The task of providing a simplified version of the ISO code of practice for the small and medium firms is now a necessity and must be taken seriously into consideration by national and international organisations on security. But until this task is accomplished, there are some other ways that SMEs can improve their practices by making use of the ISO. For example, SMEs can hire experts on the ISO 17799 and use them according to their needs. The experts on the ISO code of practice can

greatly enhance the security practices with their experience and deep knowledge on the subject. While the use of experts on ISO 17799 can help to improve the security practices within a SME, a wide range of software tools referred as ISO17799 toolkits can offer additional help towards using the document. Such tools are entirely based on the ISO17799 document and make easier the process of establishing security procedures within an organisation by using an easily approachable graphic user interface (GUI).

6. Conclusions

This paper presented the issues around security policies in small and medium enterprises. The results from various surveys conducted worldwide were found to be discouraging indicating that the majority of the small and medium companies do not follow or have difficulties in following the proper practices to secure their information system. Only a few of them reported that had a security policy in place while the money spent on security in general was minimal. For this disappointing situation there were though some reasonable factors. The lack of personnel with the proper skills and competencies is found to be the most important reason that hinders SMEs from adopting adequate security measures. It is reasonable to expect the qualified and experienced on security to seek for a career in a larger enterprise with more appealing opportunities and salaries than a small enterprise. In addition, the lack of sufficient budgets that can be justified by their small size makes less possible the chances of having security practices and particularly security policies.

Coming to a conclusion, some sort of solutions that are specific for the SME needs should be provided as these proposed in this report. The potential of using the ISO/ IEC 17799 code of practice must also be taken into consideration as a valuable and worldwide accepted solution for enterprises of any size. While the help from experts on the ISO 17799 or even the use of ISO toolkits can enhance this potentiality, a simplified version of the ISO, so that is more appealing for the SMEs, is definitely the best solution.

7. References

Briney, A. and Prince, F. (2002), “Information Security Magazine Survey – Does size matter?”, http://infosecuritymag.techtarget.com/2002/sep/2002survey.pdf (Accessed 12-Jul-2005)

Cisco Systems, Inc. (2004), “Cisco IP Communications Security Policy Development and Planning Guide”, http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/ipsug_wp.pdf (Accessed 06-Jul-2005)

DTI (2004), “Information security breaches survey 2004 technical report”, http://www.dti.gov.uk/industries/ information_security/downloads.html (Accessed 01-Mar-2005)

Ernst and Young (2004), “Global Information Security Survey 2004”, http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/$file/2004_Global_Information_Security_Survey_2004.pdf (Accessed 17-Mar-2005)

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2004), "CSI/FBI Computer Crime and Security Survey 2004", http://www.itsecurity.com/papers/insight2.htm (Accessed 12-Mar-2005)

Hamilton, C.R. (2002), "Risk Management & Security", http://www.riskwatch.com/Whitepapers/Risk_ Management_and_Security_11-07-02.pdf (Accessed 19-Mar-2005)

Hong Kong Emergency Response Team (HKCERT) Coordination Centre (2005), "Information security guide for small businesses", http://www.hkcert.org/secguide/eng/sme_guideline_e.pdf (Accessed 01-Jul-2005)

Kai, S.C., Chanson, S. and Wong, J. (2002), "E21-MagicMedia - E-security survey report", http:// www.e21magicmedia.com.hk/esecurity2002/pdf/e-Security%20Survey%20Report.pdf (Accessed 24-Jun-2004)

Melek, A. (2004), "Deloitte Touche Tohmatsu Org. - 2004 Global Security Survey", http://www.deloitte.com/ dtt/cda/doc/content/dtt_financialservices_SecuritySurvey 2004_051704.pdf (Accessed 15-Jun-2005)

Zuccato, K. (2005), "2005 Australian Computer Crime and Security Survey", http://www.auscert.org.au/ images/ACCSS2005.pdf (Accessed 16-Jun-2005)