Information Security Management in SMEs-Beyond the IT challenges

M. Sadok[1] and P. Bednar[2, 3]

[1]Higher Institute of Technological Studies in Communications in Tunis, Tunisia
[2]School of Computing, University of Portsmouth, UK
[3]Department of Informatics, Lund University, Sweden
e-mail: {moufida.sadok, peter.bednar}@port.ac.uk

Abstract

In this paper we report some results of a survey involving 33 Small and Medium-sized Enterprises (SMEs) in the UK on how they approach information security risks and what the human and organisational issues related to their risk-management practices are. All of the interviewed employees are handling sensitive data, needed to do their job, but without necessarily having the most knowledge or responsibility related to information security. The qualitative approach used was intended to be more deeply insightful and informative than others, for the purpose to understand security practices gaps, and how to improve them, as normal employees are the ones concerned with the deployment of security controls and measures in their own work practices. Our findings show that while there is a wide agreement about the importance of security and its potential impact on company performance, the understanding of security is rather taking a technology-oriented perspective. Actual work practices and routines of most employees were however ignored or not intertwined with security management efforts. Deficiencies were identified in preventive mechanisms, in incident reporting and management as well as in risk analysis process. Beyond the IT challenges, SMEs will need to have in place more efficient training and awareness programmes and organizational processes to develop more resilient security capabilities. Our conclusion is that there is a much-needed involvement of practitioners with operational knowledge in risk management and security policy definition.

Keywords

Information security, SME, Socio-technical analysis, User engagement, Security practices, Security awareness

1. Introduction

Information security management is a critical issue for SMEs as they face the same threats as big companies but with lower budget and less mature security controls. According to a PwC-UK (2015) survey 74% of small businesses recorded a security breach and the average cost of the worst breach increased to £75,200 (from £65,000 in 2014) at the lower end and the higher end had more than doubled to £310,800. In the UK, the Government's National Cyber Security Programme, launched in 2012, provides guidance and a range of tools to help businesses develop a better ability to limit the impact of security risks. For small businesses, this programme set up a number of guidelines to implement basic technical steps of security, to adopt a risk

management approach and to apply for a Cyber Essentials certificate. Once certified, SMEs could apply for the Cyber Security Incident Response Scheme. There is also a free online and introductory training course of protection against fraud and cybercrime. In the PwC-UK (2015) report, the percentage of organisations using "Ten Steps to Cyber Security" is almost one-third.

In this work, we investigate to what extent SMEs implement the Government cyber security strategy. We are particularly interested in current practices in order to identify gaps in security routines and how to improve them. A survey was conducted so as to understand security practices more fully and to provide valuable data for reflection in this research. Out of 45 invitations to local businesses in Portsmouth to participate in this survey, we received 33 positive responses (three employees were intended to be interviewed in each business). The sample was thus, essentially self-selected. These companies were drawn from a variety of sectors, including manufacturing industry, restaurants, services, and retail. The size varies from 10 to 120 employees. The research took place during the first half of 2015. In some companies we managed to interview only one employee, while in others we successfully interviewed two or three employees.

All the interviewees were handling, in different ways, sensitive data to do their job. The data are mainly related to customers and accounting services. In contrast to other surveys we did not try to contact employees with the most knowledge or responsibility related to information security management. Our objective is not to assess security practices according to a technical perspective (from IT security expert's point of view) or as described in formal policy documents. In some companies our interviewees were junior, senior, or experienced managers or officers while in other companies it might be the business owner. None of them were IT security expert as we are interested in security practices of normal employees.

The following section highlights the research methodology used. The key findings of the empirical study are then discussed in section 3. Conclusions are drawn in section 4.

2. Methodology

The interviews were guided with a questionnaire (table 1) which was discussed with each employee individually. The questionnaire is divided into five sections. It was developed taking into consideration the questionnaire addressed to small businesses within the Government's National Cyber Security Programme (available at www.gov.uk/bis) but it also covers topics with regard to human and organizational issues of information security management. We formulated closed-ended questions (the pre-determined answers are not in Table 1 due to space limitation) that reflect a practitioner perspective without necessarily having an IT background. The first three parts include respectively questions about planning, implementation and review of information security. The fourth part focuses on the scope of risk analysis while the fifth deals with organisational aspects of information security function.

Topic	Questions
Planning	What information assets are critical to your work? What kinds of risks could they be exposed to? When prioritizing security needs and developing a security practice, what are the most significant variables? How could you continue to do your job if your information requirements could not be fulfilled with your IT support? How can you manage risks and threats to your information assets on an ongoing basis?
Implementing	Have you put in place the right security controls to protect your equipment, data, IT system and external (or outsourced) services? Do you and your co-workers know what your responsibilities related to IS and cyber security are? Do you and your co-workers know what good security practices are? If there is a security threat/issue, or something goes wrong related to your information assets – how will you deal with it and get back to normal practices again?
Reviewing	Are you reviewing and testing the effectiveness of your security controls and practices? How are you monitoring and acting on the data that you receive from your security practices? How do you keep up to date with the latest security threats to your activities? Does your organization need a frequent lookout of vulnerabilities and threats? How would you describe security policy within your organization? What should the relevant reasons of security policy updating for your organization be?
Risk Management	Have you carried out a security risk assessment in your organization? While you assess risk, what would you identify?
Organization	Are responsibilities for data ownership and protection necessary to clarify in your organization? Does your organization need formally documented procedures for the management of security incident responses? Do you recommend the function of a clearly identified and attributed individual responsible for data and cyber security in your organization? What means should be deployed to enhance employees' security awareness in your organization?

Table1: Security practices questionnaire

3. Analysis of findings

Results reveal that each company has its own specific security practices, and many companies do experience different problems in the main areas of information security management. Although there is a wide consensus that data theft is the most significant risk, the ongoing management of risks and threats is mainly based on checks. These checks are in general technical and consist of simple tasks of verification of only the availability of required data to do the job. However, the unpredictability of security threats makes these checks ineffective to prevent or to keep up with evolving security risks. This is supported in the study of Dhillon and Torkzadeh (2006) where the managers interviewed have had a number of

reservations about the effectiveness of checklists and predetermined security measures.

Our survey also found that a business continuity plan is not considered in the everyday work-practices of normal employees. This result does not necessarily mean that the interviewed companies did not implement one but it means that our interviewees are not aware of or applying it. It is irrelevant in our research to confirm with companies the formal existence or not of such plan because we are interested in effective and current security practices as part of everyday work practices of normal employees.

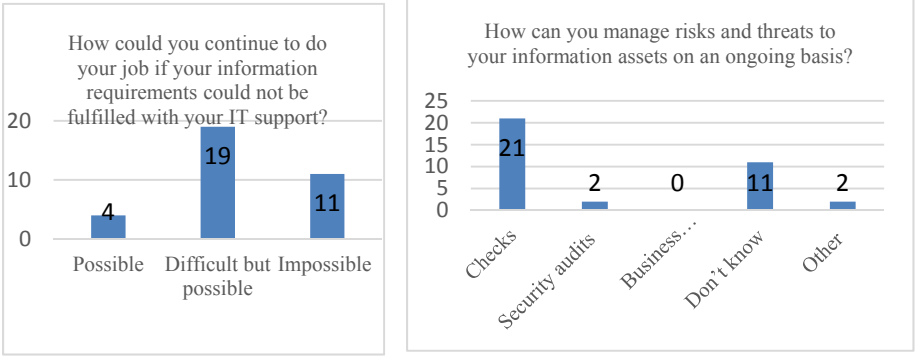

Figure 1: Information security planning practices

As noted in figure 1, the dependency on IT support is high in most of the interviewed companies to do the job. This underlines the questions of how to design secure and useable system (Sommerville, 2011) and consequently how to realize a better alignment of security checks with business objectives.

When asked about implementation practices, we noticed a relative awareness of security risks and their potential impact on job effectiveness. At an organizational level, a significant number of interviewees do not have any idea about the responsibilities related to an efficient information security management. Interestingly, our interviewees think that they are not responsible for or concerned by security as they totally rely on the IT department or on their line manger to solve problems in the case of a security threat or issue.

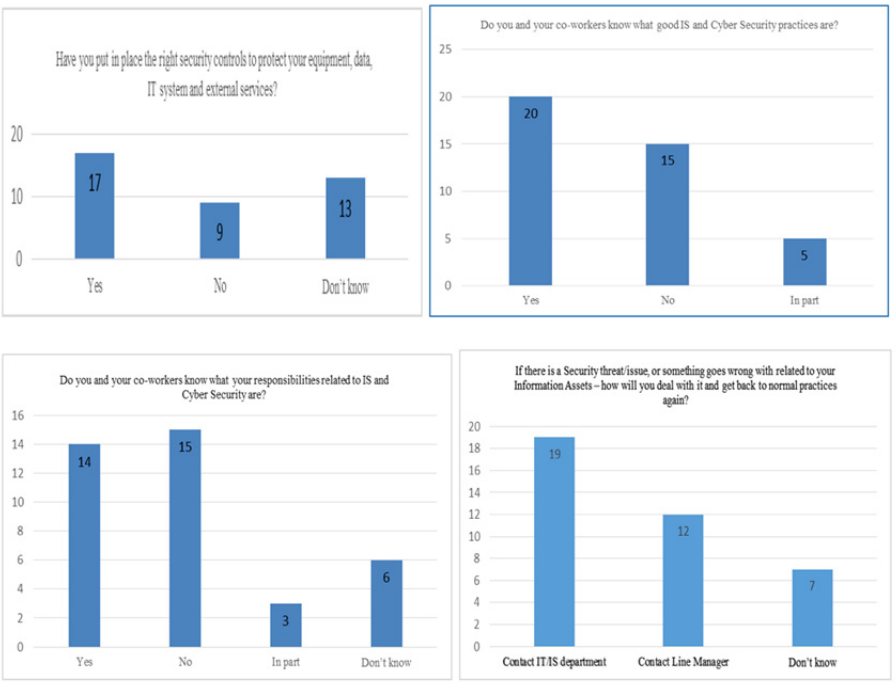

Figure 2: Implementation practices

Considering the dynamic nature of security risks, it is crucial to review and monitor on a regular bases implemented controls and procedures. The companies surveyed experience several deficiencies in their reviewing practices. It seems curious that just a quarter of respondents said that they are reviewing and testing the effectiveness of security measures. When it comes to developing proactive security capabilities, our interviewees are divided between agreement and unawareness about the usefulness of conducting a frequent lookout of vulnerabilities and threats. Based on our informal discussions with the interviewees we think that these companies are really aware of the increasing number and severity of security risks. However, in practice they do not have enough organisational and human resources to set up proactive mechanisms enabling them to detect and to shorten response to security incidents. Previous studies have also stated that lack of funds, time and specialised knowledge may explain poor security practices in SMEs (e.g. Gupta and Hammond, 2005).

Monitoring is equally crucial to check the reliability of implemented security solutions and controls. More than half of survey respondents said they did not develop formalized practices of monitoring. Only 2 respondents said that they had discussed potential changes of practices with the management and 10 cited that they file and store reports. One explanation for the relatively absence of monitoring activities and the weak engagement of operational employees in these activities may be that SMEs lack maturity in security management particularly in preventive and detective mechanisms.

We asked what means were used to keep up with security threats and risks. Publications mainly via Intranet and e-mailing are the most popular means of security awareness. Surprisingly, more than half of survey interviewees said that they did not conduct any periodic security awareness and training programs nor had security training as new employees. These results are alarming because the lack of substantive consideration of awareness and training programs by SMEs may lead to inadvertently sabotage the efficiency of implemented security solutions and procedures. We noticed when we questioned about security policy we got different answers in the same company which support the evidence that employees are not either equally aware of the existence of a security policy or how to apply its rules.

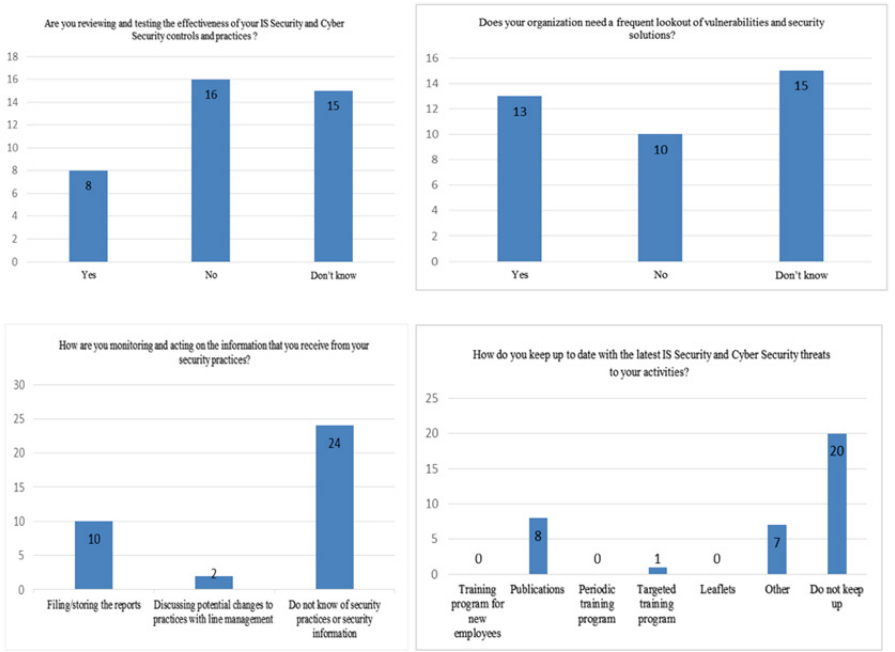

Figure 3: Reviewing practices

According to PwC-UK (2015) survey, 75% of large organisations and 31% of small businesses suffered staff-related security breaches. Furthermore, 72% of all companies where security policy was poorly understood had staff-related breaches and half of the companies attributed the cause of the single worst breach to unintentional human error. In our survey, as employees are supposed to use security policy and follow its guidelines, we purposefully asked our interviewees if they are currently applying one. Of the 39 interviewees who responded to this question, 46% reported that a formal security policy is being developed or established. Notably, just over 50% said that they don't know or apply a formal security policy. This does not necessarily mean that these companies did not define or implement a formal security

policy but it only shows that the existence of a formal security policy does not imply its efficient implementation or relevance from a practitioner perspective.

Another aspect comes out figure 4 is when a security policy is updated, it is clearly that use of new technology is prioritized. Change of work practices would be the second most important reason of security policy updating. In light of this, companies should consider processes and practices of how the contextual use of information security is involved according to a pragmatic perspective. The active engagement of users in developing information security activities contributes to more effective security measures and better alignment of security controls with business objectives (Furnell and Clarke, 2012; Bednar et al., 2013)

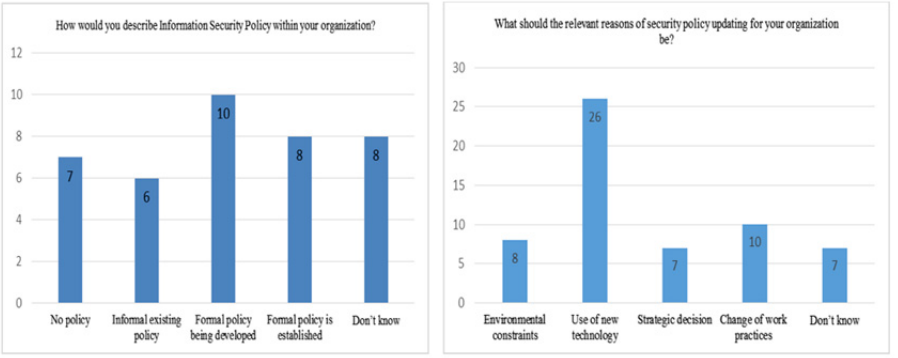

Figure 4: Security policy practices

Figure 5 illustrates the answers to the questions about risk analysis practices. Not surprisingly, approximately half of survey respondents said they do not know if their companies did carry out a security risk analysis. Almost one third of respondents said that technical system had been the focus of risk analysis These results are coherent with the findings of previous security surveys that showed a continuous focus on data system security rather than on real world organizational context as well as a prevalent involvement of top management and security staff in risk analysis process (Sadok and Bednar, 2015). However, when asked about what would be the scope of risk analysis, it appears that administrative procedures and work activities that process sensitive information followed by applications and equipment that support work activities are ranked as very important.

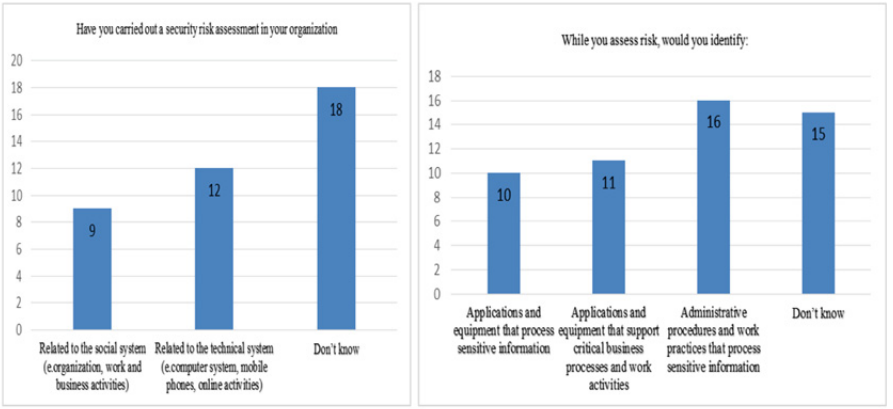

Figure 5: Risk analysis practices

Other key areas of information security management include incident reporting and mitigation, data responsibilities and ownership, and the integration of security function into the organisational structure. These organizational practices have the potential to significantly improve the ability of companies to quickly identify and respond to security incidents. Our survey identified weaknesses in all the aforementioned areas. Particularly, just over 75% of the interviewees reported that in their organizations responsibilities for data ownership and protection should be more explicit. This explains in part why two thirds advocated the necessity of having a security officer responsible for information security. In fact, the top information security officer plays a pivotal role to provide insights into risk management and to manage issues related to security incident identification, reporting and recovery. Therefore, such role requires particular skills in both business analysis and information security.

Other notable outcomes (see figure 6) include security incident response and management of business activities continuity. Since security attacks are growing in number and severity, activities such as monitoring, mitigation and investigation are essential to conduct in order to minimize the damages from security incidents. This requires the definition of a number of organizational and managerial procedures to ensure the detection of early signs of security attacks and to make appropriate decision for protecting sensitive data. Our survey respondents cited that security incident detection, mitigation and recovery are necessary practices to implement within their companies. They equally recommended the setup of a continuity plan for management of organizational operations and activities. However, just over one third don't know either the existence or the efficiency of such control and response procedures. Once again we conclude that the insufficient awareness of such security measures does not necessarily mean their absence but rather their limited relevance in context.

These findings make sense, given that SMEs have limited resources and tend to dedicate security budget to the most necessary security controls enabling them the management of an acceptable risk.

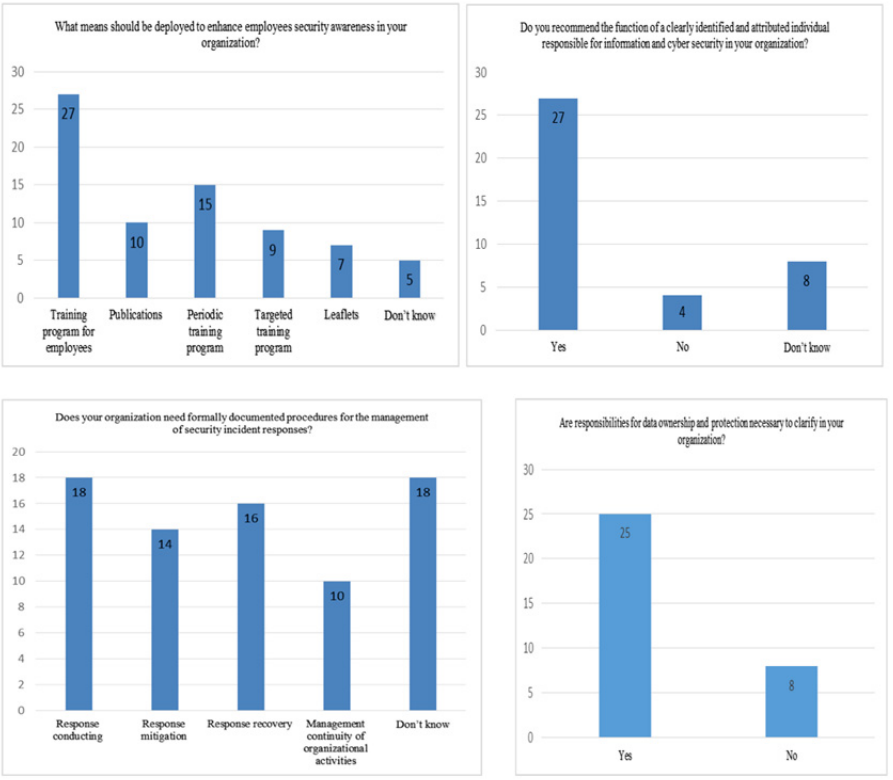

Figure 6: Organizational security practices

Information security functions are dependent on both human motivation and behaviour and infrastructural elements; hence employee training and awareness continue to be a critical component of a security strategy. Nearly 70% of survey respondents said they need ongoing security awareness and training programmes. On one hand the companies involved in this study will need to have in place more effective training programmes for improved threat awareness. On the other hand this has been the subject of a debate about the cost-effectiveness of training programmes and how to identify relevant and updated courses enabling employees to be well-prepared. Studies have outlined the trivial impact of general awareness campaigns and the lack of efficiency of generic courses based on a lecture on knowledge of security policy and procedure (e.g. Parsons et al., 2014). Given the economic impact of security breaches (Schatz and Bashroush, 2016), SMEs should consider investment decisions on security training and awareness programmes as a driven of measurable improvements in their performance results.

4. Conclusion

In terms of this study, the results can be seen as an indication of deficiencies that appear to be common in SMEs security practices and strategies that have not adequately kept up with dynamic security risks. While security practices may vary by industry and company size, the challenge for most SMEs is the integration of security function into business processes through an active engagement of all internal stakeholders in risk analysis and security policy definition. This should not be implemented as a top down managerial instruction and policy or just based on the competencies of the IT department or the security specialist.

In spite of the interest of political initiatives to support SMEs preparedness, the identified gaps in their security practices illustrate their weak understanding of how to implement and manage effective security controls and measures. SMEs may benefit from adopting a socio-technical approach to information security that streamline risk management processes, involve relevant stakeholders in operational cyber-risks mitigation and set up in place well-targeted security awareness and training programmes. Our findings also support the conclusion that security practices must be influenced by those employees who are not security experts or IT managers. If decisions on security practices remain within security expert domain, they will continue to be either irrelevant in everyday work practices or simply just unworkable.

5. References

Bednar P., Sadok M. and Katos V. (2013) “Contextual dependencies in information systems security”, Pre-ICIS Workshop on Information Security and Privacy (WISP), Italy.

Dhillon, G. and Torkzadeh, G. (2006) “Value-focused assessment of information system security in organizations”, Information Systems Journal, Vol. 16, pp 293-314.

Furnell, S. and Clarke, N. (2012), “Power to the people? The evolving recognition of human aspects of security”, Computers & Security, Vol. 31, pp 983-988.

Gupta, A. & Hammond, R. (2005) Information systems security issues and decisions for small businesses, Information Management & Computer Security, 13(4), pp 297-310.

Parsons K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014), “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)”, Computers & Security, Vol. 42, pp 165-176.

PwC-UK, 2015 UK information security breaches survey, available at www.pwc.co.uk

Sadok, M. and Bednar, P. M. (2015), “Understanding Security Practices Deficiencies: A contextual Analysis”, HAISA 2015, 151-160.

Schatz D. and Bashroush R. (2016),"The impact of repeated data breach events on organisations’ market value", Information & Computer Security, Vol. 24 Iss 1 pp. 73 - 92

Sommerville, I. (2011), Software engineering, Pearson Education Inc, ISBN: 978-0-13-705346-9.