Information Security in Hospitality SMMEs in Cape Metropolitan Area: The Management and Culture Perspective

D.S. Bedi[1] and S.C Warden[2]

[1]Faculty of Business, Cape Peninsula University of Technology, Cape Town, South Africa
[2]Faculty of Informatics and Design, Cape Peninsula University of Technology, Cape Town, South Africa
email: ds.beddy@gmail.com; wardens@cput.ac.za

Abstract

Information plays an important role in today's businesses. It needs to be protected at all costs in order to avoid facing the consequences of loss of data and compromising information. In order to address information security, SMMEs (Small Medium and Micro Enterprises) should adopt a culture that is security abiding. By supporting a security culture where members of staff intuitively protect information, SMMEs can benefit much because the employees will be aware of their responsibilities regarding information security culture. However, previous studies tend to overlook this aspect. Management of information security can also help SMMEs deal with information security breaches especially that it has been indicated that employees contribute to most of the breaches. This paper looks at the two aspects, management and culture, to find out how SMMEs in the hospitality industry can effectively use them to deal with security issues. SMMEs in the hospitality industry deal with client credit card information and they need to protect it in order to avoid the consequences.

Keywords

Information security, culture, management, policies, measures, hospitality, SMMEs

1. Introduction

SMMEs (Small Medium and Micro Enterprises) are increasingly conducting their business electronically although security has been identified as an issue, which they should contend with (Gupta & Hammond, 2005; Knapp, Morris, Marshall, & Byrd, 2009). Information can contribute to the success or downfall of a company depending on how they utilise or protect it (Thompson & Von Solms, 2005). As organisations use Information Systems (IS) as part of their business procedures, the issue of security should be carefully considered as most organisations' business processes are incorporated into each other, for example, buying and selling goods rely on IS (Kankahalli, Teo, Tan and Wei, 2003). One way of dealing with security issues is by focussing on employee's behaviour because the success or failure of a company depends largely on the actions of employees with reference to information security. Companies that emphasize and support an information security culture will reduce the risk of information compromise, especially the risk of employee misbehaviour and malicious interaction with information assets (Da Veiga & Eloff, 2010).

The dependence on information security systems requires companies to manage their security (Zuccato, 2007). Information security management is all about making sure that information is well managed, through proactive management of information security risks, threats and vulnerabilities. Information security should be included in the day to day business operations rather than being considered as an extra expense (Kritzinger & Smith, 2008).

2. Information Security

It should be emphasized that information security has evolved from dealing with minor and harmless issues to harmful security threats that can cripple a company's information systems if they are not addressed early on (Dlamini, Eloff & Eloff, 2009). Information security is an important part of a company, but the way they apply security measures, including evaluation and implementation of safeguards vary significantly. In most cases companies take wrong decisions when it comes to information security that may as a result of lack of knowledge about the security domain, threats, possible measures and the company's infrastructure (Ekelhart, Fenz, Klemen & Weippl, 2007).

2.1. Information security in hospitality SMMEs

The Internet also provides hospitality SMMEs with opportunities such as increasing their customer base, as well as improving their business operations (Kim, 2005). The price of Internet access has decreased in the past few years, making it more affordable. As a result, this has lead to more people being able to access the Internet and also increased security concerns (Heung, 2003).

A study by Trustwave, a PCI (Payment Card Industry) vendor and Qualified Incident Response Assessor issued a warning after investigating 75 cases of credit card compromise. The study revealed some interesting observations. It showed that a large number of accounts were under threat (Ragan, 2009). This is surprising because credit card leakage can result in a serious impact to these hotels as a result of the cancellation and re-issuing of the compromised cards (Dlamini et al., 2009). Most hotels that were investigated lost data that was stored on magnetic strips as a result of outdated processing systems and technologies. Because these outdated systems are used to store card information, it is easy for fraudsters to penetrate the system and download stored files. Other problems that were revealed by the study were weak passwords and improper firewall configuration, which could lead to possible security compromise (Ragan, 2009).

SMMEs in the hospitality industry are not always sure what to do in case of a security breach. Most of them do not know what to do to boost their security especially those that are connected to the Internet. Most of these SMMEs rely on limited resources and budgets and as result fail to protect their networks as well as customer information. In Singapore the government formed a Cyber Security

Awareness Alliance in order to help hospitality SMMEs with information security issues (IDA, 2008).

3. Information security culture

Culture is normally enforced by making use of rules, regulations or procedures (Von Solms', 2004). Each organisation has a culture, and through it might not be aware of this, it exists both at a conscious and non-conscious level (Vroom and Von Solms, 2004). An organisational culture is built over time by moulding behaviour within an organisation in accordance with the company's vision (Kuusisto & Ilvonen, 2003). Thompson and Von Solms (2006) indicate that the organisational culture plays an important role in influencing employee behaviour and can, therefore, be used to shape the information security behaviour of the employees. Culture is an important factor that can contribute to the success of the company since it makes everyone in the organisation to be responsible for his/her actions (Chang & Lin, 2007). Some security publications mention security as mainly a technology issue (Koh, Ruighaver, Maynard, &Ahmad, 2005; Martins & Eloff, 2002;; Von Solms', 2004), however technology can only solve part of the problems, but without a thorough change in the security culture of the company which directly influences security practices, purchasing security products will bring little success (Von Solms & Von Solms, 2004).

In cases where organisational culture in emphasized, end-users, security administrators as well as managers will be inspired to reflect on their behaviour all the time to maintain the required level of security (Ruighaver et al., 2007). In most cases, new security policies can cause a misunderstanding amongst employees and therefore introducing a policy-based security plan can prove to be a difficult task. It is therefore advisable that companies explore various traits of organisational culture for facilitating businesses in managing their information security, and moulding shared values, beliefs and norms for information security management based on the concept of organisational culture are important (Chang & Lin 2007).

3.1. Information security culture in SMMEs

In cases where organisational culture in emphasized, end-users, security administrators as well as managers will be inspired to reflect on their behaviour all the time to maintain the required level of security (Ruighaver et al., 2007). In most cases, new security policies can cause a misunderstanding amongst employees and therefore introducing a policy-based security plan can prove to be a difficult task. It is therefore advisable that companies explore various traits of organisational culture for facilitating businesses in managing their information security, and moulding shared values, beliefs and norms for information security management based on the concept of organisational culture are important (Chang & Lin 2007).

In a study conducted by Dojkovski et al. (2007), suggestions that can help SMMEs develop a security culture emerged. One way is by development and communication of related policies, procedures and responsibilities. They have noted that most SMMEs in developing countries lack these policies. The other aspect to assist these companies develop their culture is through cooperation, collaboration, sharing of knowledge and e-learning. The study further noted that in Australia currently there are no communities that support SMME employees in understanding and addressing information security issues (Dojkovski et al., 2007).

The Dojkovski et al. (2007) study also reveals that SMMEs do not have policies and procedures that build the organisation's information security culture. Companies that were involved in the study indicated that they did not have anything pertaining to information security culture (Dojkovski et al., 2007). According to Kuusisto and Ilvonen (2003) a well detailed document that outlines their security culture was only found in three SMMEs. This was also the case in the Dojkovski et al. (2007) study where all companies that participated in the research did not posses any security document.

SMMEs considered the development of strong employee values as a very difficult task (Dojkovski et al., 2007) even though some researchers have emphasized the importance of value-based behaviour as a way of developing a strong information security culture amongst all companies no matter their size (Dhillon & Backhouse, 2000; Helokunnas & Kuusisto, 2003; Martins & Eloff, 2001). The only way to succeed is to hire people who already have strong values (Dojkovski et al., 2007).

4. Information Security Management

Information security management can be defined as the part of a management system based on business risk, approach, to establish, implement, operate, monitor, review, maintain and improve information security. This definition can further be expanded by including organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources (Ashenden, 2008). It is also one way of reducing the risks to information within the company's environment by making use of security technology and management process (Chang & Lin, 2007). A trusted security technology alone cannot protect the company's information without a good management policy and implementation (Chang & Ho, 2006).

These days organisations need to collaborate with their business partners or customers. Where there is an information exchange that needs to be sent via the Internet, there will be some security problems (Von Solms, 1996). Previous studies indicate that most security issues are a result of negligence instead of attack event. The main goal of information security management is to make sure that confidence and information effectiveness within the company or between the company and its stakeholders are enhanced (Von Solms, 1996). Security is a worrying problem for all stakeholders and in order for companies to be successful in their quest to combat these threats, collaboration is needed to make sure the Internet is a secure medium that is needed for building a successful information society (Tawileh, Hilton & McIntosh, 2007).

If information security is not properly managed, it is likely to result in confusion when it comes to applying it. A likely scenario is that all risks are inadequately addressed, and some controls may not be appropriate or be over elaborate. It will thus be difficult to understand what has been done, by whom, for what reason and for what purpose without security management. Information security management will make sure that adequate and proper security measures or controls are selected that will ensure that the company's information resources are protected. Utilising information security management, the challenge of addressing the information resources will be addressed (Ashenden, 2008).

4.1. Information security management in SMEs

Managing information security seems to be a serious challenge for SMMEs and face the same challenges that as larges companies (Gupta & Hammond, 2005), but there appears to be a significant difference in the way SMMEs manage their information (Gupta & Hammond, 2005; Tawileh et al., 2007). This difference can be the result of some operational limitations faced by SMMEs which affect them as they try to apply security. Security surveys reveal that there is poor security management amongst Australian companies especially SMMEs. It has been discovered that companies do not have proper procedures and mechanisms in place to monitor security (Gupta & Hammond, 2005).

5. Data collection

Quantitative research methodology was followed for this study and preferred because the researchers wanted to confirm whether managers/owners are aware of the importance of emphasizing information security culture and information security management or not. Only people in the management of a company were considered for the study. Since respondents were mainly people in top management who are often not available, this method was selected because it provided respondents with an opportunity to objectively answer questions in their own time. The research was carried in the Cape Metropole area and only SMMEs that are connected to the Internet were considered for the study. Finally, the quantitative research methodology maintained objectivity and minimal interference by the researchers (Bryman, 1984; Kobus & Maree, 2007:145).

The survey method was used for data collection. Survey research comprises questionnaires or interviews that are used to measure current status, attitudes, values, habits and ideas from opinions and beliefs. Survey research can be categorised into two groups, namely open-ended questions and close ended questions. In this study, the questions were closed-ended. These types of questions give more precise input of data into a system, as well as for analysis purposes (Maree & Pietersen, 2007).

In order to determine SMMEs' opinion of information security, a Likert scale was used for most of the questions. This type of rating was used as it allowed the researcher to measure how SMMEs rate or emphasise information security. Options that were provided were: strongly agree, agree, unsure, disagree and strongly disagree.

5.1. Selection of the population and sample size

Participants comprised of SMMEs in the hospitality industry that conduct their business in the Cape Metropole area. The industry was selected based of the fact that tourism has grown to become one of the important sectors that contribute to economic development within South Africa. The tourism industry has been a pacesetter of new technology adoption and it offers features that render the industry well suited to e-commerce. Several countries have come to the realisation that tourism is one of the key areas to economic prosperity (Binns & Nel, 2002). Moreover, online transactions are growing at a high rate, particularly in the tourism sector (Shankar, Smith & Rangaswamy, 2003). A total of 121 questionnaires were sent to respondents and 61 questionnaires were returned. A total of 56 questionnaires were properly completed while 5 questionnaires were not used due to incomplete sections. This gives a total response rate of 47 percent. According Leedy (1997), a response rate of 47 percent is an acceptable response.

6. Empirical findings

A total of 12 percent of respondents strongly agreed that information security management minimizes information theft while 54 percent agreed to this. A total of 34 percent indicated that they are not sure whether information security management minimizes information theft. Figure 1 depicts that 11 percent of the respondents strongly agreed that accountability plays an important role when it comes to information security management. Figure 1 further depicts that a total of 59 percent agreed that accountability plays an important role when it comes to information security management while 30 percent indicated that they are not sure.

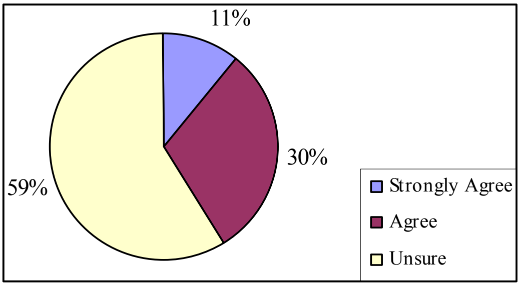

Figure 6: Information security accountability

A total of 14 percent of the respondents indicated that they strongly agree that management of information security can improve business operations while 63 percent of the respondents agreed. Those not sure whether information security management can contribute to business operations improvements comprised of 21 percent. A total of 2 percent indicated that they disagree that information security management can contribute to business operations improvement.

Policies can be used to mould the company's information security culture (Chang & Lin, 2007:440). Figure 2 depicts that 7 percent of the respondents indicated that they strongly agree they have information security policies in place to deal with security breaches while 41 percent indicated that they agree. Those not sure whether their companies possess information security policies comprises 16 percent. Figure 2 further depicts that 36 percent of the respondents indicated that their companies do not have any security policies in place to enforce security in the minds of employees.

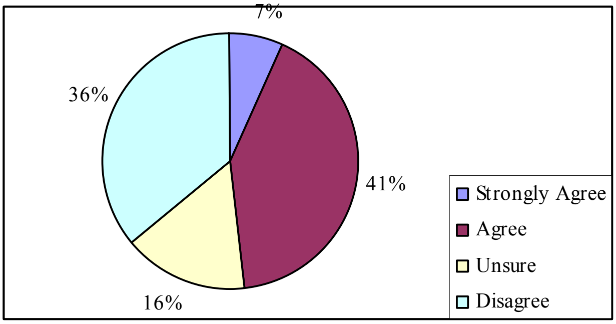

Figure 7: Information security policy possession

Only 9 percent of the respondents indicated that they strongly agree that their policies are understandable to their employees while 41 percent of the respondents indicated they agree. Of the respondents, 16 percent indicated that they are not sure whether their policies are understandable to their employees. A total of 30 percent of the respondents indicated that they disagree that their policies are understandable to their employees and therefore making them useless. Only 4 percent indicated that they strongly disagree that their policies are understandable to the employees. On the other hand, a total of 2 percent of the respondents indicated that they strongly agree that their information security policies are accessible to staff members while 27 percent indicated that they agree. A total of 27 percent indicated that they are not sure whether their policies are accessible to staff members or not. A total of 44 percent of the respondents indicated that they disagree that information security policies are accessible to staff members.

Of the respondents, 19 percent indicated that they strongly agree that employees are encouraged to follow the security measures in place to deal with security breaches. Even though 59 percent indicated that they encourage their employees to follow security measures in place in order to avoid being a victim of security breach, it is still worrying. On the other hand, 10 percent indicated that they are not sure whether staff members are encouraged to follow security procedures or not. A total of 18 percent of the respondents indicated that they disagree that they encourage their employees to follow the measures in place.

Training can play an important role in instilling information security culture into the minds of the staff members (Ruighaver et al., 2007). It seems some SMMEs in the Cape region do not believe in training new employees. Figure 3 depicts that 9 percent of the respondents strongly agreed that they provide training to the new employees while 49 percent indicated that they agree. Figure 3 depicts that a total of 27 percent of the respondents indicated that they are not sure whether their companies provide training or nor to the new employees. Figure 3 depicts that a total of 13 percent indicated that they do not provide training to the new employees and therefore leaving themselves vulnerable to the employees' mistakes. A total of 2 percent indicated that they strongly disagree that they provide training to the new employees. It is very surprising because a total of 4 percent of the respondents indicated they strongly agree that they have suffered a loss as a result of employee mistakes while total of 18 percent indicated they agree. A total of 32 percent indicated that they are not sure whether their companies have suffered a loss as a result of employee mistakes. On the other hand, a total of 32 percent of the respondents indicated have never suffered a loss as a result of employee mistakes. A total of 18 percent indicated that they strongly agree that they have never suffered a loss as a result of employee mistake.

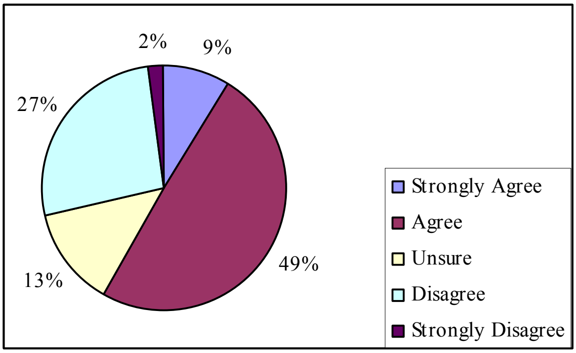

Figure 8: Security training in SMMEs

The roles of all the employees should be clearly defined so that there won't be any duplication of tasks in the company. According to Ashenden (2008:197), if roles are properly defined, information security will be adequately addressed and managed. It seems SMMEs in the Cape Metropole area do not heed his advice. Most of the respondents (59 percent) indicated that roles in their companies are not clearly defined while 12 percent indicated that they do not know whether roles are clearly defined within their company or not. Only 27 percent of the respondents indicated that roles are clearly defined in their companies.

7. Conclusion

Even though a majority of the respondents indicated that they agree that information security management can minimise information security theft, there are still some hospitality SMMEs indicated that they are not sure whether information security management can help in terms of curbing security breaches especially by staff members. This shows that some SMMEs do not emphasize information security management and this can be disastrous to the company's information resources. There are some SMMEs that do not believe that information security management can contribute to business operations. A sizeable number of the respondents indicated that they are not sure whether information security management can improve their business operations.

One way of enforcing a security culture is using information security policies and training. Such policies will make employees aware of what is expected of them; therefore a culture abiding staff-base will be created. However, it is important to note there are some SMMEs that do not have any security policies. These businesses are creating a culture that is responding to security breaches rather than creating a culture that is security proactive and therefore abiding to the company' s security practices. A number of SMMEs indicated that they do not have any security policies in place and this can expose their information resources. Without security policies, employees won't know what is expected of them in terms of information security. Policies should also be made accessible and understandable to staff members in order to make sure that they serve their purpose.

Employees should always be encouraged to follow the provided guidelines or measures in place to make sure that they avoid security breaches. Some respondents indicated that they do not encourage their employees to follow security measures in place. This can cause businesses a loss of revenue due to security breaches if security is not enforced. Training can also assist SMMEs to enforce their information security culture especially to new employees. New employees need a thorough induction in order to know how information is held in the company. There are some SMMEs that do find it necessary to train new employees and this can be very disastrous for the company. Lastly, this study proved that SMMEs in the hospitality industry do not emphasize security abiding culture which explains why these companies experience security breaches. Finally, it was noted that information security management does not exist amongst SMMEs.

8. References

Ashenden, D. 2008. Information security management: A human challenge. Information security technical report, 13(2008):195-201.

Binns T. & Nel, E. 2002. Tourism as a local development strategy in South Africa. South African geographical journal, 168(3):235-247.

Bryman, A. 1984. The debate about quantitative and qualitative research: A question of method or epistemology? The British journal of sociology, 35(1):75-92.

Caralli, A. W. & Wilson, R. W. 2004. The challenges of information security: Survival enterprise management team. www.cert.org/archive/pdf/ESMchallenges.pdf [Accessed 20 March 2009].

Chang, S.E. & Lin, C.H. 2007. Exploring organisational culture for information security management. Industrial management and data systems, 107(3):438-458.

Chang, S.E. & Ho, C.B. 2006. Organisational factors to the effectiveness of implementing information security. Industrial Management and data systems, 106(3):341-351.

Da Veiga, A. & Eloff, J.H.P. 2010. A framework and assessment instrument for information security culture. Computers and security, 29(2010):196-207.

Dhillon, G. and Backhouse, J. 2000. Technical opinion: Information system management in the new millennium. Communications of the ACM, 43(7):15-128.

Dimopoulos, V., Furnel, S.M., Jennex, I. & Kritharas, I. 2005. Approaches to IT security in Small and medium enterprises. Proceedings of the 2nd Australian information security management conference, Perth. Australia.

Dlamini, M.T., Eloff, J.H.P. & Eloff, M.M. 2009. Information security: The moving target. Computers and security, 28(2009):189-198.

Dojkovski, S., Lichstein, S. & Warren, M. 2007. Developing information security culture in Small and Medium size Enterprises. Proceedings of the 6th European Conference on information Warfare and Security, Shrivenham, 2-3 July 2007. Defence College of Management and Technology.

Ekelhart, A., Fenz, S., Klemen, M. & Weippl, E. 2007. Security ontologies: Improving quantitative risk analysis. Proceedings of the 40th Hawaii International Conference on Systems Sciences. 3-6 January. Waikoloa, Island.

Gupta, A & Hammond, R. 2005. Information systems security issues and decisions for small businesses. Information management and computer security, 13 (4):297-310.

Heung, V.C.S. 2003. Internet usage by international travelers. International journal of contemporary hospitality management, 15(7):370-378.

Hone, K. & Eloff, J.H.P. 2002. What makes an Effective Information Security Policy. Network Security, 20(6):14-16.

IDA. 2008. Need a helping hand to beef up security? http://www.ida.gov.sg/Infocomm%20Adoption/20090317161523.aspx [Accessed 10 April 2009].

Kankahalli, A., Teo., H.H., Tan., B. C. & Wei, K. K. 2003. An intergrative study of information systems security effectiveness. International journal of information management, 23 (2):139-154, April.

Kelleher, D. 2009. SME security: SME mindset must change. http://www.scmagazineus.com/sme-security-sme-mindset-must-change/article/136052/ [Accessed 21 June 2009]

Kim, C. 2005. Enhancing the role of tourism SMEs in global economic value chain: A case analysis on travel agencies and tour operators in Korea. Proceedings of the 2005 Conference on Global Tourism Growth: A challenge for SMEs. Gwanju, 6-7 September 2005, Korea: Kyunghee University:1-19.

Knapp, K. J., Morris, R.F., Marshall, T.E. & Byrd, T.A. 2009. Information security policy: An organisational level process model. Computers and security, 28(2009):493-508.

Kobus, K. & Maree, K. Questionnaire design. In Maree, K. 2007. First steps in research. (ed). Pretoria:Van Schaik:154 -170.

Koh, K. Ruighaver, A.B. Maynard, S.B. and Ahmad, A. 2005. Security governance: Its impact on security culture. http://scissec.scis.ecu.edu.au/anzsys08/proceedings/2005/aism/koh.pdf [Accessed 27 January 2009].

Kritzinger, E. & Smith, E. 2008. Information security management: An information retrieval and awareness model. Computers and security, 27(2008):224-231.

Kuusisto, T. and Ilvonen, I. 2003. Information security culture in small and medium size enterprises. http://www.ebrc.info/kuvat/431-439.pdf [Accessed 10 December 2009].

Lange, T. Ottens, M. & Taylor, A. 2000. SMEs and barriers to skills development: a Scottish perspective. Journal of European industrial training, 24(1):5-11.

Leach, J. 2003. Improving user security behaviour. Computers and security, 22(8): 685-692.

Leedy, P.D. 1997. Practical research: Planning and design. Upper Saddle River, NJ: Prentice Hall.

Martins A. and Eloff, J. 2002. Information Security Culture. Proceedings of the 17th International Conference on Information Security (SEC2002), Cairo, (2002). 7-9 May, Kluwer Academic Publishers Group, Netherlands: 203–214.

Mishra, S. & Dhillon, G. 2006. Information systems security governance research: A behavioral perspective. http://www.albany.edu/iasymposium/2006/mishra.pdf [Accessed 22 January 2010].

Olnes, J. 1994. Development of security policies. Computers and security, 13(3):628-636.

Posthumus, S. & Von Solms, R. A framework for the governance of information security. Computers and security, 23(8):638-646.

Ragan, S. 2009. Security vulnerabilities persist in hospitality industry. http://www.thetechherald.com/article.php/200921/3719/Security-vulnerabilities-persist-in-hospitality-industry [Accessed: 10 February 2010].

Ruighaver, A.B., Maynard, S.B. & Chang, S. 2007. Organizational security culture: Extending the end-user perspective. Computers and security, 26(2007):56-62.

Shankar, V., Smith, A. K & Rangaswamy, A. 2003. Customer satisfaction and loyalty in online and offline environments. International journal of marketing, 20(2):153-175.

Stanton, J.M. Stam, K.R. Mastrangelo, P. & Jolton, J. 2005. Analysis of end user security behaviors. Computers and security, 24(2):124-133, July.

Stokes, A. 2001. Using telementoring to deliver training to SMEs: a pilot study. Education and training, 43(6):317-324.

Tawileh, A., Hilton, J. & McIntosh, S. 2007. Managing information security in Small and Medium Sized Enterprises: A holistic approach. http://www.tawileh.net/anas//files/downloads/papers/InfoSec-SME-ISSE.pdf?download [Accessed 12 February 2010].

Thompson, K.L. & Von Solms, R. 2005. Information security obedience: A definition. Computers and security, 24(1):69:75.

Von Solms, B. 2000. Information security-The third wave? Computers and security, 19(7):615-620.

Von Solms, B. & Von Solms, R. 2006. Information security governance: A model based on the Direct-control cycle. Computers and security, 25(2006):408-412.

Von Solms, B. & Von Solms R. 2004. The 10 deadly sins of information security management. Computers and security, 2004(23):371-376.

Von Solms, B. & Von Solms, R. 2004. From policies to culture. Computers and security, 2004(23):275-279.

Von Solms, R. 1996.Information security management: The second generation. Computers and security, 15(4):281-288.

Vroom, C. & Von Solms, R. 2004. Towards information security behavioral compliance. Computers and security, 23(3):191-198, May.

Zuccato, A. 2007. Holistic security management for framework applied in electronic commerce. Computers and security, 26(3):256-265, May.