



PROCEEDINGS OF THE
11th ANNUAL CONFERENCE
ON WORLD WIDE WEB APPLICATIONS

2-4 September 2009
Port Elizabeth
South Africa

Editor:
P.A. van Brakel

Publisher:
Cape Peninsula University of Technology
PO Box 652
Cape Town
8000

Proceedings published at
<http://www.zaw3.co.za>

ISBN: 978-0-620-45215-1

TO WHOM IT MAY CONCERN

The full papers were refereed by a double-blind reviewing process according to South Africa's Department of Education (DoE) refereeing standards. Papers were reviewed according to the following criteria:

- Relevancy of the subject to Web applications
- Explanation of the research problem & investigative questions
- Quality of the literature analysis
- Appropriateness of the research method(s)
- Adequacy of the evidence (findings) presented in the paper
- Standardised referencing style.

The following reviewers took part in the process of evaluating the full papers of the 11th Annual Conference on World Wide Web Applications, held from 2 tot 4 September 2009 in Port Elizabeth:

Prof J Brits
Faculty of Information Sciences (Dean)
University of Wisconsin
Milwaukee
USA

Prof T Carr
Centre for Higher Education Development
University of Cape Town
Cape Town

Prof J Cronjé
Faculty of Informatics and Design (Dean)
Cape Peninsula University of Technology
Cape Town

Mr Craig de Beer
Web Management Services
Massey University
Palmerstone
New Zealand

Prof M Erasmus
Management Information Systems
Erasmus Associates
Lynnwood
Pretoria

Dr AM El-Sobky
Educational Sciences
RITSEC
Cairo
Egypt

Dr MWH Labour
Laboratory of the Sciences of Communication
University of Valenciennes and Hainaut Cambrésis
Valenciennes Cedex
France

Prof S Mutula
Department of Information Science
University of Botswana
Botswana

Dr David Raitt
European Space Agency
The Hague
The Netherlands

Prof A Singh
Department of Business Information Systems
University of KwaZulu-Natal
Durban

Prof P Weimann
Economics and Social Sciences
University of Applied Sciences
Berlin
Germany

Further enquiries:

Prof PA van Brakel
Conference Chair: Annual Conference on WWW Applications
Cape Peninsula University of Technology
Cape Town
+27 21 469 1015 (landline)
+27 82 966 0789 (mobile)

Web security in hospitality SMMEs: investigating policies and measures in the Cape Metropole area

D.S. Bedi
Faculty of Business
Cape Peninsula University of Technology
Cape Town, South Africa
202056600@cput.ac.za

S.C. Warden
Faculty of Informatics and Design
Cape Peninsula University of Technology
Cape Town, South Africa
wardens@cput.ac.za

SMMEs¹ have often been confined to particular geographical locations to carry out their business. Recently SMMEs have become increasingly more location independent and they are finding it strategically advantageous operating in more than one location made possible by the interconnectivity of the web. The web now offers SMMEs even more opportunities but at the same time, are faced by the challenge of ensuring that adequate measures are in place to protect their information. They therefore, need to protect their information being a valuable asset. The advances in modern technology, especially in the case of computers connected to the web resulted in SMMEs being more vulnerable to loss or the compromise of information due to malicious activity. Most SMMEs in the hospitality industry are required to be connected to the web in order to compete effectively in the market but also face serious consequences if they do not have adequate precautions in place to protect their information. Furthermore, SMMEs are not always aware of the risks that they are exposed to while customers for example, expect some degree of protection when dealing with online businesses. The aim of this paper is to conduct a preliminary study to investigate to what extent SMMEs in the hospitality industry have security policies and measures in place to firstly, keep their information secure and secondly, what security their customers would expect. From this investigation, the researchers will be able to ascertain to what extent SMMEs are generally exposed to in an effort to propose guidelines how to effectively deal with these challenges in their quest to secure their information.

Introduction

Organisations and businesses are increasingly using the web for business and it has been identified that security is an important issue to contend with (Gupta & Hammond, 2005:297). Furthermore, the use of Information Systems (IS) as part of business procedures is not exempt as the security issues also need to be carefully considered (Kankanhalli, Hai-Teo & Wei 2003 :139). This leads to the realisation that most organisations' business processes are closely related to each other for example, buying

¹ Countries use different definitions for SMEs and are referred to SMMEs in South Africa
Proceedings of the 11th Annual Conference on World Wide Web Applications, Port Elizabeth,
2-4 September 2009 (<http://www.zaw3.co.za>)

and selling goods relying on IS. Zuccato (2007:256) is of the opinion that IS needs to be protected by means of information processing security systems.

Flowerday and Von Solms (2005: 605) define information as the "...oxygen of the modern age" while many organisations rely on information for their success (Navaro, 2001:29; Geber & Von Solms, 2001:581) rather than on physical devices and services (Flowerday & Von Solms, 2005:605). As information forms the backbone of most businesses but stored in different formats for example, it can be stored in computer systems, sent via the web, saved as a soft copy, sent as facsimiles, stored on tapes or compact disks and can be sent by email. Gerber and Von Solms (2001:581) conjure that no matter in what format information is stored; it does need to be protected to avoid unauthorised disclosure, manipulation, modification or destruction. Whittman and Matford (2005:8) view web information security as the protection of information and its supporting elements, including the systems and hardware that use, store and transmit information. The main goal of information security is to ensure that an organisation's information, as stated before being an important asset, is not disclosed to unauthorised persons especially in the hospitality industry where credit card information needs to be kept secure (Wiant, 2005:451).

Law, Leung and Wong (2004:100) indicate that escalation of tourism services and products together with a high increase in tourism demand have resulted in the adoption of a wide variety of IT products, especially the web which has contributed to the success of this industry. These authors state that the web is a new communication and distribution means for e-travellers and suppliers of hospitality services and products. Furthermore, Maswera, Edwards and Dawson (2008:12) point out that e-Commerce enabled by the web can be used to improve tourism in Africa. This can be enhanced by the vast amount of wildlife, unique resorts and fauna to generate extra revenue from international markets. They further found that the web has proved to be a useful tool in the tourism industry as it was used to increase revenue in developed countries. Trading on the web is also cost effective as Martin (2004:83) found in the USA and Canada that hospitality SMEs describes the web as a cheaper means of advertising especially accessible by clients from all over the world. The study that was carried by Warden (2007:226) indicates that trading on the web does not only provide SMMEs with an opportunity for a quick response but it also offer a new trading opportunity by providing an online environment that satisfies the expectations of customers. Even though trading on the web has got some advantages, it also has its own downfalls (Lee, 2002:76).

According to Miyakazi and Fernandez (2001:28) government and organisations by and large have identified information confidentiality and security, to be the main factors that prevent companies from conducting business on the web. The authors further indicate that risk perceptions associated with web privacy and security has been identified as the main worrying issues concerning online users. According to Zheng, Caldwell, Harland, Powell, Woerndl and Xu (2003:35), SME in the UK were are cautious when using online business because they believe that it makes them transparent and therefore become vulnerable to information theft. The study further revealed that SME were unwilling to adopt online business being concerned that trading over the web threatened their uniqueness and ability to personalise their market offerings. This would be done by influencing the interpersonal relationship based SMEs business models. Similarly, Peterson, Meinert, Criswell and Crossland (2007:656) reveal that trust issues contribute

to consumers not being interested in conducting business on the web, more especially with SMEs.

Background

Importance of SMMEs to the South African economy

SMEs play a critical role in the upliftment of economies especially in developing countries (Zindiye & Mwangolela, 2007:90; Thurik & Wennekers, 2004:141). Their contribution to a country's national product is significant either producing goods of value, providing services to consumers or to other enterprises (Adele, 2004:4). The World Bank has also noted the role played by SMEs in developing countries and therefore has embarked on financing support programs for SMEs (Beck, Dermiguc-Kunt & Levine, 2005:199). While one country might define an SME as an enterprise that has less than five hundred employees, another country might define it as an enterprise that has less than two hundred and fifty employees (Ayyagari, Beck & Dermiguc-Kunt 2007:415). In South Africa, SMMEs are defined according to the industry that they operate and in the catering and accommodation industry, they are enterprises that:

- have a total financial turn over of less than 64 million rand per year
- have total assets of 10 million rand excluding fixed assets
- employs less than 200 hundred people (South Africa, 2003)

SMMEs are vital to the South African economy and can be a valuable source of employment and mechanism for the process of upgrading human capital (Dallago, 2004:18). Similarly to Europe where a number of countries have used SMEs as a platform towards industrialisation and economic development, South Africa can use SMMEs as a tool to curb unemployment (Adele, 2004:4). Zindiye and Mwangolela (2007:90) indicate that small emerging firms can play a major role in South Africa since the formal employment opportunities are not increasing as expected.

Web information security

Many companies have realised that in order to compete effectively in the business environment, they need to protect information as well as their supporting systems (Chang & Hong, 2006:345, Fulford & Doherty, 2003:106). Kankanhalli, Hock-Hai, Bernard and Kwok–Kee (2003:140) indicate that increased reliance on Information and Communication Technologies (ICT) especially the web has resulted in an increase impact of security abuse. Furthermore, Bojanc and Jerman-Blazic (2008:217) postulate that in most cases threats are focussed to attack information as well as its supporting systems. The types of threats are escalating and have been increasing ever since the development of computers and the interconnection of the web (Gerber, Von Solms, & Overbeek, 2001:33). A successful attack on a company's network can result in system crashes and eventually loss of data, services and business operations (Clear, 2007:2, Bojanc & Jerman-Blanzic, 2008:216). These threats have resulted in companies

investing more on security measures and data protection devices (Bojanc & Jerman, 2008:216, Fulford & Doherty, 2003:106). This action has resulted in companies spending more on security products pointed out by Fulford and Doherty (2003:106). Belanger, Hiller and Wanda (2002:246) add by indicating that unless security issues are addressed fully, consumers will not be motivated to conduct business on the web.

It has been indicated that a sizeable number of the consumers are concerned about threats to their privacy (Brown & Muchira, 2004:63). Violations of privacy can affect the company negatively, for example the company might experience a decline in the stock prices (Acquisti, Friedman & Telang, 2006: 5).

Web Information security of Hospitality SMMEs

Earlier studies indicate that the hospitality industry is mostly affected by credit card scam than any other industry. This was verified by an investigation carried out by Trustwave, a PCI vendor and Qualified Incident Response Assessor. A warning was issued after the investigation of 75 cases of credit card compromise. The study revealed some interesting observations. It showed that over one million accounts were under threat. The study further indicated that most of the hotels that were investigated lost data stored on magnetic strips as a result of outdated processing systems and technologies. These outdated systems used to store credit card information, makes it very easy for fraudster to penetrate systems by downloading stored files. Other issues revealed in the study were weak password strategies and improper firewall configurations leading to possible security compromise (Ragan, 2009).

Most of the SMMEs in the hospitality industry are unsure how to address web security, especially those connected to the web. They rely on limited resources and budgets and therefore sometimes fail to protect their networks and customer information. In Singapore, the government formed a Cyber Security Awareness Alliance in order to help SMEs with information security issues (IDA, 2008).

Web information security in SMMEs

The issue of security of SMMEs has been debated over the past number of years. Analysts indicate that SMMEs need to be protected similarly to the case of larger companies (Chapman & Smalov, 2004:5). Chapman and Smalov (2004:5) warn SMEs to understand the risks associated with World Wide Web. In a study that was conducted by Chapman and Smalov, (2004:5) of the 500 managers, it was found that 61 percent of SMEs had no firewalls, while 76 percent had some anti-virus software installed on their systems. SMEs are misinformed if they believe that hackers are only targeting large companies (Millard, 2007, Morgan, 2006:3, Park, Robles, Hong, Yeo & Kim, 2008: 92). This however, is not the case because large companies have usually put strong web security measures in place as a result of government demands on security. Cyber criminals are therefore often turning to SMEs being easy targets because in most cases their web is not guarded (Morgan, 2006:3). This is supported by Kim, Lee and Lee (2006) indicating that 74 percent of all hacking took place with SMEs. However, SMEs continue to ignore computer breaches, leaving themselves vulnerable to such attacks.

Despite the evidence indicating that phishing attacks are on the rise and becoming more sophisticated, about 62 percent of SMEs did not have any form of protection in place to curb these kinds of attacks. Furthermore, employees in SMEs are likely to be overloaded with junk mail as almost 50 percent of SMEs did not have web filtering system in place giving employees the opportunity to access any website, anytime on the day, resulting in low productivity (Chapman & Smalov, 2004:5).

Web security policies

Peterson et al. (2007:658) indicate that privacy policy outlines how personal information will be handled. The above authors further add that the privacy policy statement can be used a tool to increase the customers' trust. According to Hone and Eloff (2002:15), an effective web security policy can be used to influence users to adjust their behaviour in order to ensure that a company's reputation is not at stake. These authors further state that a policy must be able to take both, user's and business needs into consideration to have the desired effect. In so doing, users will be convinced that web security is not a threat, but rather a procedure taken to ensure that the business information is protected (Hong, Chi, Chao, Tang, 2006:105). If a policy is understandable, employees can more easily refer to it when faced with difficult situations therefore, not wasting time by consulting management and others (Luzwick, 2001:16, Hong *et al.*, 2006:105). Furthermore, user's rights and responsibilities will be properly defined via policies (Hong *et al.*, 2006:105).

According to Gupta and Hammond (2005:299) most SMEs do not have policies and measures in place thus making them more vulnerable to attacks. In most cases they do not have any documentation to guide their employees in terms of security practices or policies (Park *et al.*, 2008: 92). Upfold and Sewry (2005:2) are in agreement indicating that it is surprising that a lack of policies is common amongst SMEs, even though business connection to public networks is increasing. This is supported by the study that was conducted by Dojkovski, Lichstein and Warren (2007:1566) indicates that 82 percent of SMEs do not have any policies in place to monitor their information assets.

Methodology

Amaratunga, Baldry, Sarshar Newton (2002:22) reveal that quantitative research can be described by the assumption that human behaviour which can be referred to as "social facts", can be investigated using methodologies that make use of "the deductive logic of natural sciences". This opens the way to follow a quantitative research methodology and accordingly, a quantitative methodology was followed for this research. A survey research design was preferred over other methods providing an opportunity to obtain detailed and consistent descriptions of both policies and measures used by SMMes (Peterson *et al.*, 2007:660). This research design allowed the respondents to answer the questions objectively since they were given an opportunity to answer at their own time. The questionnaires were hand delivered after the respondents were contacted telephonically or via email.

Sample Size

The sample was made up of SMMEs in the Hospitality industry conducting their business in the Cape Metropole area that are conducting their business on the web. The Cape Metro Council (1999:4) defines the Cape Metropole as the area that is well known for its florist nature and covers an area of 2 175 square kilometres. It is located between the Table Mountain and the Hottentonts Holland mountains and surrounded by the Atlantic Ocean (Cape Metro Council, 1999:4). A total of 100 questionnaires were distributed to Hospitality SMMEs in the Cape Metropole area. The data collection was carried out over a period of 5 months (January – May). A total of 47 SMMEs participated in this study.

Results and discussion

In this section the findings of the preliminary research concerning SMMEs in connection with information security is discussed. The results are presented under the following headings;

- Formal steps outlining the necessary procedure to report web security
- The company deploys adequate web security policies
- Web security
- Security measures in place to protect information

The results indicate that 63.8 percent of respondents rely on outsiders for their IT maintenance even though 82 percent of the SMMEs that took part in the survey have suffered data loss of some sort. The most common problem experienced by SMMEs is virus infection (82.5 percentage) followed by loss of data that was not backed up (32 percent). Even though virus infection is a persisting problem, SMMEs still prefer to store their information on current systems. Of the respondents, 59 percent prefer to back up their data on the system and 20 percent of the respondents indicated that their back up was done off-site. This supports the notion that local SMMEs still lack an understanding of web information security. The results further vindicate the previous studies conducted in Australia indicating that SMEs do not make use of IT managers (Dojkovski *et al.*, 2007:1667), Dimopoulos, *et al.*, 2004, Gupta & Hammond, 2005). Dojkovski *et al.*, (2007:1568) indicate the lack of IT managers might force SMMEs to opt for a reactive rather than proactive measure towards information security.

Formal steps outlining the necessary procedure to report web security incidents

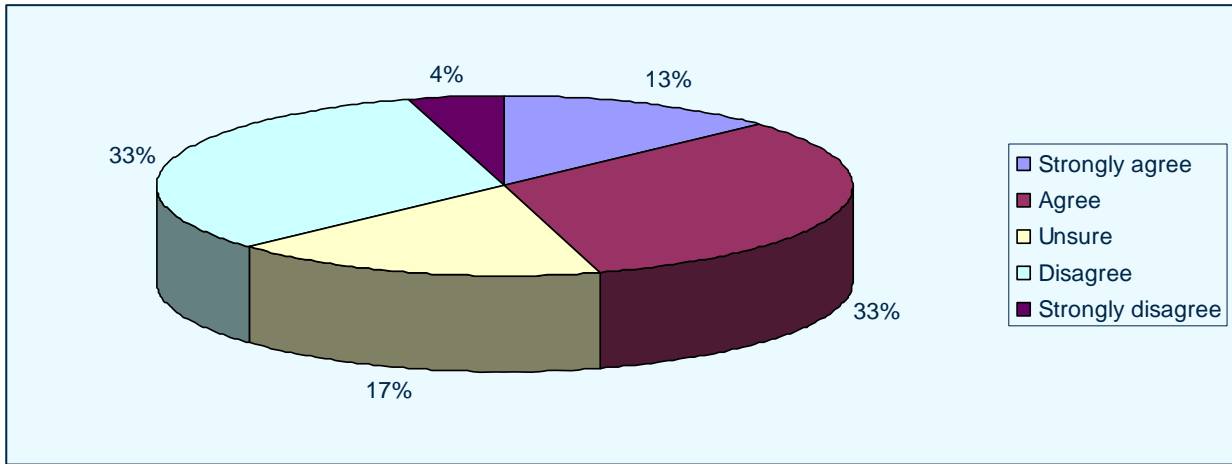


Figure 1: The necessary procedure to report web security

From the findings depicted in Figure 1 it can be conjured that SMMEs do not consider web security to be an important aspect or that they are ignorant when it comes to web security. This is demonstrated by a sizeable number of the respondents who indicated that they do not have any procedure in place. Furthermore, 33 percent of the respondents agreed that there were no procedures in place while 4 percent strongly disagreed. This gives a total of 37 percent of SMMEs in Cape Town that are vulnerable to information theft. On the other hand, 17 percent of the respondents were unsure whether there were procedures in place to report information security. Less than half of the respondents indicated that they have a procedure in place to report information security. Finally a total of 33 percent indicated that they agreed with the above statement and 13 percent strongly agreed.

The company deploys adequate web security policies

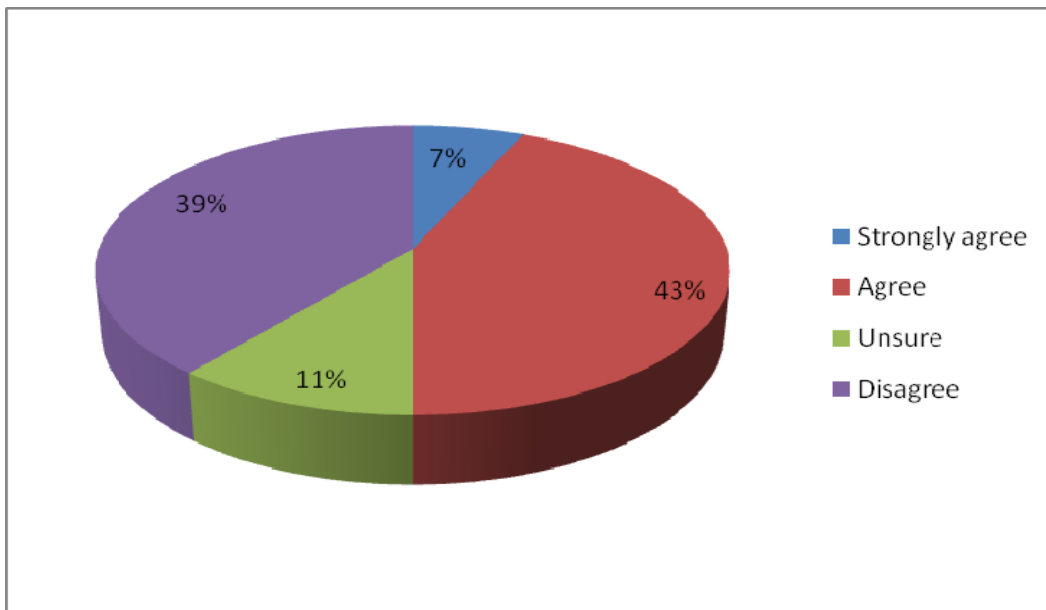


Figure 2: Web security policies chart

The results reveal that 39 percent of the respondents depicted in Figure 2 did not have

any web security policies in place to ensure that information is protected while 11 percent of the respondents were unsure whether their companies had policies. This might influence customers not to conduct business on the web with these SMMEs. Even though half of the respondents responded positively as indicated by 43 percent who agreed and 7 percent who strongly agreed, it is noted that 50 percent of respondents who indicated that they have a web policy in place, they stated that they do not review their policy on a regular basis. Of these respondents 45 percent indicated that they do not review their information web security policies on a regular basis, whereas 28 percent of SMMEs indicated that they review their web policies on a regular basis and 21 percent indicated that they were not sure whether their policies were reviewed on a regular basis. The study further indicated that 53 percent of the respondents did not have a password policy in place. This means that users do not have a guideline on how to protect their passwords and how to deal with web issues. This may result in exposing the SMMEs information systems as no policy is available to guide them in terms of password formulation. As Zviran and Haga (1999:165) indicated, organisations should form password policies that will not be easy to remember and also not easy to be guessed. This is not the case found with SMMEs in Cape Town because most of them indicated that they do not have any password policy in place.

Web security is a worrying factor in our company

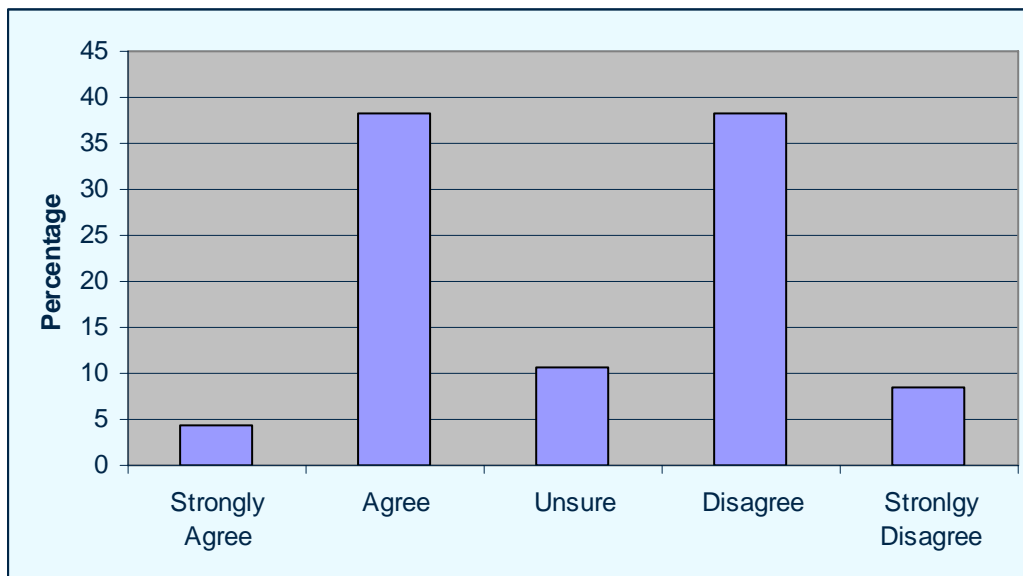


Figure 3: Internet problems

Figure 3 depicts that SMMEs in Cape Town have web issues that are worrying them. This has been revealed by the high number of respondents who indicated that they are still sceptical when it comes to web connection. The study indicates that 4 percent of the respondents strongly agreed while 38 percent agreed that web security is a worrying factor. Furnell (2004:10) indicates that an increase in the web connection has also resulted in an increase in the number of security issues. Despite this concern SMMEs still fail to take the necessary precautions to ensure that their webs are secure. On the other hand, 47 percent of the respondents were not bothered by the web security as indicated by 9 percent who strongly disagreed and 38 percent who disagreed while 10 percent of the respondents were not sure.

Web security measures in place to protect information

The results reveal that 18 percent of the SMMEs do not use any ICT device as a means of security. They indicated that elementary security systems such as anti-virus software are not used. As a result, this leaves them vulnerable to attacks. Of the respondents, 80 percent indicated that they have some devices in place to protect their information. Even though a bigger percentage SMMEs indicated that they have devices in place, they do not carry weakness assessment on a regular basis to determine if their devices are effective. The results indicate that 45 percent of SMMEs do not carry out weakness assessment to determine if there are any weaknesses on the network. On the other hand, 27 percent of the respondents were unsure whether an assessment was conducted. Finally, 28 percent indicated that they check their networks to determine if there are any weaknesses.

Conclusion and recommendations

Even though web usage has increased, it is interesting to note that in actual reality it does not translate to high consumer spending. Consumers are still reluctant to buy goods online especially from SMMEs. Privacy plays an important role in e-commerce and most of the consumers still believe that their privacy is at risk especially when conducting business on the web with SMMEs. The issues of privacy and security need to be addressed fully in order to convince consumers to conduct online business with SMMEs. Confidentiality also play an important role in web security because consumers will always do business with companies that they trust that they will hold their details in confidence and only be used in ethical ways.

SMMEs seldom have a password policy in place to guide employees how to formulate passwords. This makes them more vulnerable to attacks. Although SMMEs indicated that one of their key challenges is lack of finance to cater for security challenges, they need to take security more seriously. This paper revealed new insights for example; SMMEs do not value the input of end-users in web security. Considering that most of the SMMEs have one or two managers, they need to involve end-users when formulating their policies. This will in turn improve their security.

It is recommended that SMMEs should start by training their employees to keep up with on-going security challenges. Technology keeps on changing and therefore it is very important that employees are equipped so as to cope with its demands. Most of the Hospitality SMMEs conduct online bookings; they need to provide training to their staff to avoid costly mistakes. In most cases, the Hospitality SMMEs conduct online bookings while their customers expect their credit card information to be kept secure. Customers expect a certain degree of protection from the SMMEs whenever they conduct business with them. They do not expect their information to be revealed to third parties without their consent.

The most common problem that SMMEs are facing is virus infection. This might be

caused by lack of knowledge by end-users because they are not provided with training. Another reason why SMMEs might experience this problem is because they do not update their anti-virus software on a regular basis. Viruses are not as malicious as hacking, but they can contribute to poor productivity because they tend to slow the system. They can also cause the system crashes if not detected early. This would result in loss of finance. Back up procedures should also be conducted off-site to avoid loss of critical information. It is clear from this study that SMMEs generally adopt a reactive rather than proactive measure in their security matters.

References

Acquisti, A., Friedman, and Telang, R. 2006. Is there a cost to privacy breaches? An event study. *Proceedings of the 20th International conference on information systems*. Milwaukee. United States of America. 10-13 December.

Amaratunga, D., Baldry, D., Sarshar, M. and Newton, R. 2002. Quantitative and Qualitative research in the built environment: application of mixed research approach. *Work Study*, 51(1):17-31.

Ayyagari, M., Beck, T. and Dermiguc-Kunt, A. 2007. Small and medium enterprises across the globe. *Small business economics*, 29(4):415-434.

Baskerville, R. and Siponen, M. 2002. An information meta-policy for emergent organisations. *Logistics and information management*, 15(5):337-446.

Beck, T., Dermiguc-Kunt, A. and Levine, R. 2005. SMEs, Growth and Poverty: Cross-Country Growth. *Journal of economic growth*, 10 (2):199-229.

Belanger, F. Hiller, S.J., and Smith, W.J. 2002. Trustworthiness in the electronic commerce: the role of privacy, security and site attributes. *Journal of strategic information systems*, 11 (2):245-270.

Bojanc, R. and Jerman-Blazic, B. 2008. Towards a standard approach for quantifying ICT security investment. *Computer standards and interfaces*, 30(4):216-222, May.

Chang, S. and Ho, C.B. 2006. Organisational factors to the effectiveness of implementing information security management. *Industrial management and data systems*, 106(3):345-361

Chapman, D. and Smalov, L. 2004. On information security guidelines for Small/Medium Enterprises. *Proceedings of 6th International conference on enterprise information systems*, Porto. Portugal. 14-17, April.

Clear, F. 2007. SMEs, electronically-mediated working and data security: cause for concern? *International journal of business science and applied management*, 2(2):1-19.

Dallago, B. 2004. The importance of SMEs in transitional economies. http://www.humancapitalinstitute.org/hci/tracks_small_medium_enterprises.guid?currentTab=researchTab [09 September 2008].

Flowerday, S. and Von Solms, R. 2005. Real time information integrity = systems integrity + data integrity + continuous assurances. *Computers and security*, 24 (8):604-613, October.

Fourie, L.C.H. 2003. The Management of Information security – A South African case study. *South African journal of business management*, 34(2):19-29, May.

Fulford, H. and Doherty, N.F. 2003. The application of information security policies in UK based organisations: an exploratory investigation. *Information management and computer security*, 11(3):106-114.

Furnell, S. 2004. E-Commerce security: a question of trust. *Computer fraud and security*, 2004(10):10-14, October.

Gerber, M. and Von Solms, R. 2001. From risk analysis to security requirements. *Computers and security*, 20(7):577-584, October.

Gerber, M., Von Solms, R. and Overbeek, P. 2001. Formalizing information security requirements. *Information management and computer security*, 9(1):32-37.

Gilmore, A., Gallagher, D. and Henry, S. 2007. E-marketing and SMEs: operational lessons for the future. *European business review*, 19(3):234-247.

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

Hong, K.S., Che, Y.P., Chao, L.R. and Tang, J.S. 2006. An empirical study of information security on security elevation in Taiwan. *Information management and computer security*, 14(2): 104-115.

Kankanhalli, A., Hock-Hai, T., Bernard, C. Y. T. and Kwok-Kee, W. 2003. An integrative study of information systems security effectiveness. *International journal of information management*, 23(2):139-154, April.

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

Kim, H.S., Ahn, M.H., Lee, G.S. and Lee, J. 2006. The information security guideline for SMEs in Korea. <http://ww1.ucmss.com/books/LFS/CSREA2006/SAM3066.pdf> [22 January 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.

Law, R., Leung, K. and Wong, J. 2004. The impact of the Internet on travel agencies. *International journal of contemporary hospitality management*, 16(2):100-107.

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

Lee, P.M. 2002. Behavioural model for online purchasers in e-Commerce environment. *Electronic commerce research*, 2(2):75-85.

Luzwick, P. 2001. Information warfare attacks are a concern, then evaluate the security policy. *Computer fraud and security*, 2001(9):16-19, September.

Lybaert, N. 1998. The information use in SMEs: its importance and some elements of influence. *Small business economics*, 10(2):171-191.

Martin, L. 2004. E-innovation: Internet impacts on small UK Hospitality firms, *International journal of contemporary hospitality management*, 16(2):82-90.

Maswera, T., Edwards, J. and Dawson, R. 2008. Recommendation for e-commerce systems in the tourism industry of sub-Saharan Africa. *Telematics and informatics*, 26 (1), December 17.

Millard, E. 2007. How vulnerable is your SME? <http://www.processor.com/editorial/article.asp?article=articles/P2922/20p22/20p22.asp> [22 November 2008].

Morgan, R. 2006. Information Security for small businesses. http://www.infosecwriters.com/text_resources/pdf/Information_Security_for_Small_Businesses.pdf [20 July 2008].

Miyakazi, A.D. and Fernandez, A. 2001. Consumers' perceptions of privacy and security risks for online shopping. *The journal of consumer affairs*, 35(1):27-44.

Morgan, B. 2004. 2010: Real benefits off the field. http://www.southafrica.info/2010/2010_wc_thoughts.htm [21 August 2007].

Navarro, L. 2001. Information security risks and managed security services, *Information security technical report*, 6 (3):28-36, October.

Park, J. Y., Robles, J.R., Hong, C.H., Yeo, S. and Kim, T. 2008. IT security strategies for SMEs. *International journal of software engineering and its applications*, 2(3):91-98.

Peterson, D., Meinert, D., Criswell II, J. and Crossland, M. 2007. Consumer trust: privacy policies and third-party seals. *Journal of small business and enterprise development*, 14(4):654-669.

Ragan, S. 2009. Security vulnerabilities persist in hospitality industry. <http://www.thetechherald.com/article.php/200921/3719/Security-vulnerabilities-persist-in-hospitality-industry> [20 May 2009].

Shapshak, T. 2009. Be prepared: Computers can be replaced, data can't. *Sunday Times*: 8, June 14.

Sharma, M.L. and Bhagwat, R. 2006. Practice of information systems: Evidence from select Indian SMEs. *Journal of manufacturing technology management*, 17(2):199-223.

South Africa. 2003. National Small Business Amendment Act. Notice 26 of 2003. *Government gazette*, 461:1-10.

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

Thurik, R. and Wennekers, S. 2004. Entrepreneurship, small businesses and economic growth. *Journal of small business and enterprise development*, 11(1):140-149.

Ward P. and Smith, C.L. 2002. The development of access control policies for information technology systems. *Computers and security*, 21(4):356-371, August.

Warden, S.C., 2007. E-Commerce adoption by SMMEs – How to optimise the prospects

of success. Unpublished Doctor's dissertation. Cape University of Technology. Cape Town

Upfold, C.T. and Sewry, D.A. 2005. An investigation of information security in small and medium enterprises in Eastern Cape. Unpublished Master's dissertation. University of Pretoria. Pretoria.

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

Wen, H.J. and Tarn, J.H.M. 1998. Internet security: a case study of firewall selection. *Information management and computer security*, 6(4):178-184.

Whittman, M. and Matford, H. 2005. 2nd Ed. Principles of Information Security. Thompson Publishing

Wiant, T. 2005. Information security policy's impact on reporting security incidents. *Computers and security*, 24(6):448-459, September.

Zheng, J., Caldwell, N., Harland, C., Powell, P., Woerndl, M. and Xu, S. 2004. Small firms and e-business: cautiousness, contingency and cost benefits. *Journal of purchasing and supply management*, 10(1):27-39, January.

Zindiye, S. and Mwangolela, T. F. 2007. Entrepreneurship a key to poverty reduction and socio-economic development. *Proceedings of the 2007 Conference: On SMMES development: an African perspective*, 12-14 September 2007. Pretoria: University of Pretoria: 88-98.

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

Zviran, M. and Haga, W. 1999. Password security: An empirical study. *Journal of management information systems*, 15(4):161-185.