Code of Ethical Practice and Cyber Security of Cloud Context: A Study Perspective of IT Authorities in SMEs.

Ruwan Nagahawatta
Centre for Cyber Security Research and Innovation.
RMIT University
Melbourne, Victoria
Email: r.nagahawatta@deakin.edu.au

Matthew Warren
Centre for Cyber Security Research and Innovation.
RMIT University
Melbourne, Victoria
Email: matthew.warren2@rmit.edu.au

Abstract

The purpose of this paper is to explore Code of Ethics practices in relation to cyber security in the Cloud context relating to small and medium-sized enterprises (SMEs). The study was based on primary data collected via a questionnaire focusing on the Australian Computer Society (ACS) Code of Ethics and its relationship to Cloud computing. The survey was aimed at Australian SMEs. The results of the research confirmed the importance of Code of Ethics in relation to professional development and professionalism.

Keywords: Cyber security, SMEs, ACS, Code of Ethics and Cloud computing.

1. Introduction

Technological, organisational, and human elements are equally important in being able to integrate cyber security and adequately secure data. Both security and privacy in relation to technology in organisations are critical to ensuring cyber security. However, security in technology and security in organisations are significantly connected to security in human (Safa et al. 2016). Unlike traditional information systems, Cloud computing refers to the enabling of on-demand computing resources. These Cloud computing resources use a service approach that move data to external resources managed by third parties. Cloud computing

offers many advantages for businesses (Marston et al. 2011; Alshamaila et al. 2013; Gupta et al. 2013), but there are many security and privacy challenges that may hinder their acceptance (Doherty 2015; Arafat 2018; Bhuiyan et al. 2019). Small and medium-sized enterprises (SMEs) play an important role in the economic development of any nation (Wong and Aspinwall, 2004). The small and medium enterprise sector has received increasing and significant attention from governments, within Australia Australian SMEs comprise 95% of businesses, accounting for 70% of Australian employees and over 57% of Australian Gross Domestic Product (GDP) contribution (ABS, 2018). There are three types of Australian SMEs: micro businesses that have less than 4 employees; small businesses with 5 to 19 employees; and medium businesses with 20 to 199 employees (ABS, 2012). However, there are limited studies examining the ethical practices in Cloud usage by SMEs. Therefore, the focus of this paper is on Australian SMEs understanding the Australian Computer Society (ACS) code of ethical practices. This study employed a quantitative approach to examine how the ACS Code of Ethics relate to Australian SMEs and their cloud practices. This study will provide an insight to determine how the ACS code of ethical practices could influence Australian SMEs in their use of Cloud computing.

2. Why should SMEs use Cloud computing?

SMEs generally vary from large enterprises in terms of their capacity, structure, and size of the business. Cost is a key issue for SMEs, as they have limited financial resources to spend on their IT facilities. Therefore, this contributes to the problems that SMEs face: lack of IT resources, lack of IT professionals and security systems (Doherty 2015). However, SMEs have some advantages in terms of close communication between employees and managers and their capability to execute and implement decisions quickly. SMEs can use Cloud computing for a variety of different applications, such as corporate website, content management system (CMS), email, internal payroll processing, customer relationship

management (CRM), and the archiving of internal corporate documents. Cloud computing can offer many business benefits for SMEs especially, as its services are most often “pay as you go”, which can be an attractive cost structure for SMEs; it also enables software that avoids an upfront investment in hardware (Senarathna et al. 2018). The overall cost for Cloud adoption is often less than the cost needed to function with traditional IT solutions (Dekker and Liveri 2015). Online collaboration is often easier in the Cloud environment as access is warranted to users of various end-user devices, at different physical locations, and it offers advantages in relation to information security and networking.

Larger Cloud service providers (CSPs) can deliver advanced security measures, whilst spreading connection costs across many customers. On the other hand, potential security and privacy settings could be shared between customers or be translated into some specific security advantages such as Cloud security auditing, standard security interface, and data backup (Dekker and Liveri 2015). Further, many Cloud computing applications such as email and file storage are widely used by SMEs. Cloud computing offer initial benefits for SMEs who are attempting to use innovative computer applications, in a cost-effective manner (Skafi et al 2020). Many SMEs are incapable of managing their own IT infrastructure but have an adequate IT budget in accordance with their usage and requirements. Therefore, SMEs can reduce their capital expenditure for IT infrastructure by utilising and paying for the services and resources provided by the Cloud computing environment (Rittinghouse and Ransome 2017). Cloud computing offers appropriate business models and even adopts a combination of different business models to improve the performance of their businesses. In addition, Cloud computing can provide for SMEs’ needs as indirect and direct “pay as you go” models, and it seems to be a more suitable choice for many SMEs due to its flexible budget arrangements and scalability (Sultan 2011). Therefore, Cloud computing offers significant benefits and opportunities for many SMEs.

3. Case Study: Compromise of an Australian SME with national security links

In November 2016, the Australian Cyber Security Centre (ACSC) identified that an Australian SME network had been attacked by a malicious cyber adversary and that SME had links to national security projects. According to the ACSC analysis, the adversary attacker had access to the SME network for a long period of time and had downloaded a vast amount of data. The analysis show that the adversary was able to gain the access to the company's network misusing an internet-facing server, and then had moved across the entire network with the support of administrative credentials. This enabled the attacker to install multiple web shells in the victims' network; a script was uploaded to a webserver empowering remote administration of the machine, to gain and maintain further access. An investigation revealed that 'sensitive data was freely accessible due to seemingly no encryption or access control measures being in place, so sensitive data was found to be freely accessible due to the apparent absence of encryption or access control measures. The key finding was that the SME did not correctly configure the security features of the systems they had (ACSC Threat Report, 2017).

4. The Cloud Computing Survey from the perspective of SMEs

This paper uses a quantitative research approach to identify the influence of cyber security and Code of Ethics related factors influencing the use of Cloud computing in Australian SMEs. Quantitative research method involves measurements and the statistical analysis of data collected through a surveyed questionnaire (Blaikie 2009). Innovation adoption studies are well defined, and several theories and models have been validated and developed to survey the acceptance of new innovations (Tehrani & Shirazi 2014). A study design is a plan that provides the procedural outline for the conduct of the study (Amedahe 2004). The study described in this paper adopted a standard questionnaire technique to collect data. The research design is reliable according to Sarantakos (2004), is a standard method of data

collection in which information is gathered through an online questionnaire. The unit of analysis for this study is an Australian SME. The study also included a wide geographical distribution of SME across the states and territories in Australia. Accordingly, the target population for this quantitative study consisted of decision makers (IT managers or decision makers in the IT section or other authorities) from different types of SMEs in Australia, who were responsible for and authorised to make policy decisions and technology acquisition for their business. Survey respondents were asked to identify which of the ACS Code of Ethics principles that focused on the ACS Code of Ethics practices in a Cloud context. The distribution of the respondents is shown by table 1.

	Frequency	**Percentage**	**Valid Percentage**	**Cumulative Percentage**
IT related authorities				
Owner	95	32.9	32.9	32.9
Chief Executive Officer (CEO)	23	8.0	8.0	40.8
Chief Information Officer (CIO)	18	6.2	6.2	47.1
Chief Security Officer (CSO)	11	3.8	3.8	50.9
IT Manager	46	15.9	15.9	66.8
IT Executive	57	19.7	19.7	86.5
Other	39	13.5	13.5	100.0
Number of employees				
1-4 (micro)	151	52.2	52.2	52.2
5-19 (small)	85	29.5	29.4	81.7
20-199 (medium)	53	18.3	18.3	100.0
State/Territory				
NSW	81	28.0	28.0	28.0
VIC	75	26.0	26.0	54.0
QLD	52	18.0	18.0	72.0
WA	36	12.5	12.5	84.4
SA	23	8.0	8.0	92.4
TAS	11	3.8	3.8	96.2
NT	4	1.4	1.4	97.6
ACT	7	2.3	2.3	100.0
Use of Cloud computing				
Yes	176	60.9	60.9	60.9
No	113	39.1	39.1	100.0

Table 1. Demographic characteristics of responding organisations.

The study sample has 289 responses, which forms the basis for the data analysis (Table 1). The demographic statistics of these responses was analysed based upon the, organisation size, business operate state or territory, and Cloud usage. Table 1 presents the descriptive statistics are used to summarise the demographic features of data. The employment profile of the respondents was examined, a minority of the respondents (33%) held ownership positions of the SMEs. The remaining of the sample (67%) were CEO (7%), CIO (15%), CSO (4%), IT manager (8%), IT executive (20%), and other (13%). According to the organisational profile based on the total number of employees, 52% of the respondents were from organisations which employed 1 to 4 employees (micro), 30% employed 5 to 19 employees (small) and 18% employed 20 to 199 employees (medium). The Australian states with the larger populations provided the higher response rates. From the sample collected, 28% of the respondents were from New South Wales (NSW), Victoria (VIC) (26%; n=75), Queensland (QLD) (18%; n=52). The remaining SMEs came from Western Australia (WA) (12.5%), South Australia (SA) (8%), Tasmania (TAS) (3.8%), Northern Territory (NT) (1.4%), and the Australian Capital Territory (ACT) (2.3%). The number of SMEs which used Cloud computing was high, more than half (60.9%; n=176) of responding SMEs identified as being current users of some form of Cloud computing service. The survey of the 289 SMEs showed there were also motivations and concerns for the use of Cloud computing.

5. ACS code of ethical practices perspective of IT authorities

The Australian Computer Society (ACS) has a code of professional conduct. The ACS Code of professional conduct is reflected with the six principles within the Code of Ethics (Australian Computer Society 2014), which are:

- "The Primacy of the Public Interest: You will place the interests of the public above those of personal, business or sectional interests;

- The Enhancement of Quality of Life: You will strive to enhance the quality of life of those affected by your work;
- Honesty: You will be honest in your representation of skills, knowledge, services and products;
- Competence: You will work competently and diligently for your stakeholders;
- Professional Development: You will enhance your own professional development, and that of your staff;
- Professionalism: You will enhance the integrity of the ACS and the respect of its members for each other."

According to the research results, as shown in Figure 1, the ethical code with the highest response was honesty, 26%, then the primacy of public interest was next with 21%. However, the improvement in quality of life and skills responded to 17% and 16% respectively. Given that the number of IT professionals is lower in SMEs due to their size, there was only a 12% response for professionalism and the lowest response was 8% for professional development.

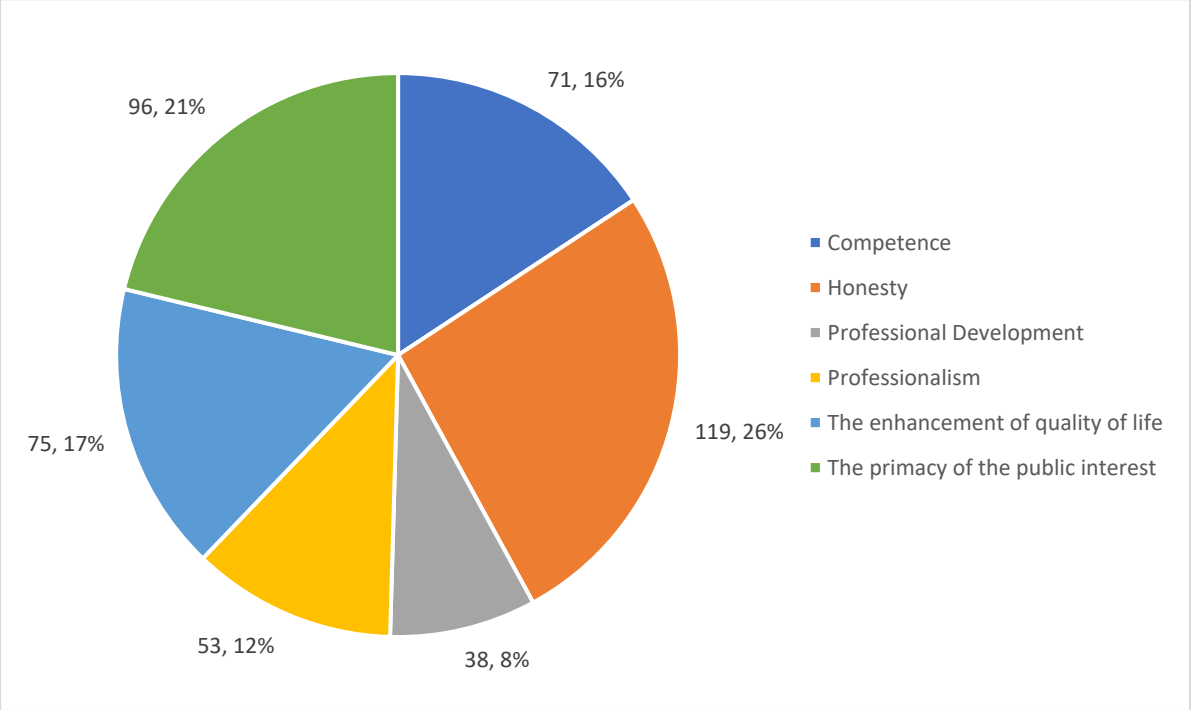

Figure 1. ACS Code of Ethics practices

6. Discussion and Conclusion

The concept of Cloud computing and the benefits for SMEs were briefly discussed. A survey of 289 SMEs showed their motivations and concerns in using Cloud computing services. The survey results show that SMEs are highly interested in Cloud computing, which enables them to improve accessibility, reduce costs, scalability, and flexibility. These advantages are seen by SMEs as key factors in using Cloud computing services. However, the rapid growth of business data, located in the Cloud, has raised issues related to cyber security, vendor lock-in, and complications with privacy and data protection. Consequently, as a result, this has led to slow growth in the use of Cloud computing.

The Code of Ethics is an important feature defining the ethical behaviour that an organisation expects of its employees. Most large organisations have a Code of Ethics that sets out their basic principles, values, and desired behaviour. However, SMEs may not have its own set of codes with respect to ethics concerned. As specified by the ACS ethical code of conduct professional development is an important aspect of ethical behaviour. Due to various reasons including the fear of being sacked, employees might choose not to report a cyber incident especially if it is caused by their negligent behaviour. Not reporting an incident can be considered ignorance. For example, not escalating an incident would make it difficult to contain it leading to the spread of malware throughout a network, compromising sensitive information. As a result of unethical behaviours SMEs could face many risks such as the loss of reputation, profits and the decline of employee morale. Further, this study found that two of the ACS Code of Ethics namely professional development and professionalism could leave SME more open to cyber threats rather than the large organisations particular in a Cloud context. Therefore, Codes of Ethical practice are related to cyber security and can provide necessary condition of address issues for the use of Cloud computing in SMEs.

This research has been limited by the ACS Code of Professional Conduct specified by the ACS. The future direction of research can focus on case studies to explore awareness of cyber security and Code of Ethics play in the practical problems of SMEs. Further, future studies can contribute on what can be done to mitigate cyber threats and ethical issues by reducing these concerns and proposing the best practices.

7. References

Alshamaila, Y., Papagiannidis, S., and Li, F. 2013. "Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework*," Journal of Enterprise Information Management,* (26:3), pp. 250–275.

Arafat, M. 2018. "Information security management system challenges within a cloud computing environment," *in Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, pp. 60. ACM.

Australian Bureau of Statistics (ABS), 2012. Australian Small Business – Key Statistics and Analysis. Retrieved from, https://static.treasury.gov.au/.../AustralianSmallBusinessKeyStatisticsAndAnalysis.pdf

Australian Bureau of Statistics (ABS), 2018. "Business use of IT and Innovation in Australian Businesses," Retrieved from: 2020, www.abs.gov.au/ausstats/abs@.nsf/mf/8166.

Australian Computer Society, 2014. "Code of Professional Conduct", Retrieved from, https://www.acs.org.au/

Australian Cyber Security Centre (ACSC), 2018. ACSC 2017 Threat Report Retrieved from: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

Blaikie, N. 2009. "Designing Social Research," Polity, Cambridge.

Bhuiyan, M.Y., Othman, S.H. and Radzi, R.Z.R.M. 2019. "An Enhancement of TOE Model by Investigating the Influential Factors of Cloud Adoption Security Objectives*," International Journal of Innovative Computing*, (9:1).

Dekker, M. and Liveri, D. 2015. "Cloud security guide for SMEs," *European Union Agency for Network and Information Security*.

Doherty, E., Carcary, M., and Conway, G. 2015. "Migrating to the cloud: Examining the drivers and barriers to adoption of cloud computing by SMEs in Ireland: an exploratory study," *Journal of Small Business and enterprise development,* (22:3), pp. 512–527.

Gupta, P., Seetharaman, A., and Raj, J. R. 2013. "The usage and adoption of cloud computing by small and medium businesses," *International Journal of Information Management*, (33:5), pp. 861–874.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. "Cloud computing - the business perspective," *Decision support systems,* (51:1), pp. 176– 189.

NIST, S., 1998. 800-16, National Institute of Standards and Technology (NIST). "Information Technology Training Requirements: A Role-and Performance-Based Model", NIST Special Publication 800-16.

Rittinghouse, J. W. and Ransome, J. F. 2017. "Cloud computing: implementation, management, and security," CRC press.

Safa, N. S., Von Solms, R., and Furnell, S. 2016. "Information security policy compliance model in organizations," *Computers & security*, (56), pp. 70–82.

Sarantakos, S., 2004. Deconstructing self-defense in wife-to-husband violence. The Journal of Men's Studies, 12(3), pp.277-296.

Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., and Salzman, S. 2018. "Factors that influence adoption of cloud computing: An empirical study of Australian SMEs," *Australasian Journal of Information Systems*, (22).

Skafi, M., Yunis, M.M. and Zekri, A., 2020. "Factors Influencing SMEs' Adoption of Cloud Computing Services in Lebanon: An Empirical Analysis Using TOE and Contextual Theory," *IEEE Access*, (8), pp.79169-79181.

Sultan, N.A. 2011. 'Reaching for the 'cloud': How SMEs can manage', *International Journal of Information Management*, (31:3), pp 272-8.

Tehrani, S. R. and Shirazi, F. 2014. "Factors influencing the adoption of cloud computing by small and medium size enterprises," *in International Conference on Human Interface and the Management of Information*, pp. 631–642. Springer.

Wong, K. Y., & Aspinwall, E., 2004. 'Characterizing knowledge management in the small business environment', *Journal of Knowledge Management*, (8:3), 44-61. Retrieved from, http://dx.doi.org/10.1108/13673270410541033

Acknowledgements

This research was supported by the RMIT International Tuition Fee Scholarship and the RMIT University Centre for Cyber Security Research and Innovation (CCSRI).