Journal of Engineering and Applied Sciences 12 (16): 4150-4155, 2017
ISSN: 1816-949X

Security Compliance Behaviour of SaaS Cloud Users: A Pilot Study

[1, 2]Hanifah Abdul Hamid, [1]Mokhtar Mohd Yusof and [3]Nuradli Ridzwan Shah Mohd Dali
[1]Faculty of Information and Communication Technology,
University Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia
[2]Faculty of Science and Technology,
[3]Islamic Finance and Wealth Management Institute (IFWMI), Universiti Sains Islam Malaysia,
Bandar Baru, Nilai Negeri Sembilan, Malaysia

Abstract: In the SaaS cloud environment, information security has been a major hindrance. Technical solutions are abundant however, it is still insufficient to protect information from intruders. Study shows that a significant number of security incidents are caused by human error be it intentionally or accidently. Security incompliance has been identified to make up one fourth of the security problems in the cloud environment and has caused a paramount loss of income and valuable data in the organisation. Drawing on cognitive theory and organisational theory, this study aims at developing a conceptual framework by identifying relevant human factors which give impact to the security conduct of the employees in the organisation. Employing a mixed method approach a pilot study was conducted to test the reliability of the developed model. Result shows the significance and reliability of all items tested hence a development of conceptual framework.

Key words: Security compliance behaviour, culture, software as a servicecloud computing, assessment, preliminary study, items, tested

INTRODUCTION

Computer scientists have been creating various technical solutions to overcome security hindrance. The introduction of password encryption, biometrics, anti-virus protection to name a few may reduce a number of security breaches but yet, security incidents still happen all the time. Information security in the cloud is much challenging than the traditional Information System (IS) due to the fact that cloud is a shared computing environment. Security threats are everywhere and the risks are higher. Studies on cloud landscape show that security has been a major obstacle of information systems in the cloud environment (Abdul Hamid and Yusof, 2016). There are many factors influencing security breaches but human errors-intentionally or accidently, add 39% contribution to the security incidents in the organisations (Connolly and Lang, 2013). Security incompliance has been identified to make up 22% of the security problems in the cloud environment (Gonzalez *et al*., 2012). Security incompliance has caused a paramount loss of income and valuable data in the organisation (Castro, 2013; Miller *et al*., 2015). The security incidents put the organisation's integrity at stake which eventually jeopardise its business opportunities. Kayworth and Whitten (2012) argued that technical solutions need to be complemented with human approach to enhance information security. Technical solutions may be effective to prevent security breaches from the outside but not from the within. This is the reason why technical paradigm alone is not sufficient to protect information in the cloud environment. This study will address the gap of security compliance issue from the human perspective. Hence, the objective of this study is to identify all of these socio-organisational factors affecting information security compliance of SaaS users and to develop a model of information security compliance behaviour. The current progress of the research is seeking to answer these research questions:

- What are the social factors which give impact to the security compliance behaviour of SaaS users in the organisation?
- What are theorganisational factors which give impact to the security compliance behaviour of SaaS users in the organisaion?

Thereotical framework: The framework is proposed to be based on social cognitive theory and organisational theory. The social aspect is further divided into three

Corrresponding Author: Hanifah Abdul Hamid, Faculty of Information and Communication Technology,
University Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia

factors-personal, behavioural and environmental factors. Social Cognitive Theory (SCT) posits that human behaviour is bidirectionally influenced by the individual values as well as the surroundings environment (Bandura, 1989). Organisation theory is phrased for a reference of topics related to organisation structure, organisation environment, power, influence and strategy (Donaldson, 1985) which form the organisational culture. The organisational aspect takes into consideration the security governance and management factor inclusive of organisational culture.

Factors influencing security behaviour

Personal values factor: Individuals were born with their own personal traits. Some of these traits are inherited from the ancestors but others may be developed depending on the how they are raisedup. For instance if a child is brought up with very strict rules and punishment they will grow up being a rebellious. The personal values may influence the way they see things and behave towards one issue including security issue. Existing research has proven that personal characteristics give impact towards the security culture of the organisation (Alfawaz *et al*., 2010; Connolly *et al*., 2015). The employee's ethical belief (Al-Hamar *et al*., 2010; Herath and Rao, 2009; Van Niekerk and Von Solms, 2010), attitude (Safa *et al*., 2015), security (Alfawaz *et al*., 2010; Van Niekerk and Von Solms, 2010; Zakaria, 2006) and level of trust (Al-Hamar *et al*., 2010; Colella *et al*., 2014; Safa *et al*., 2016) play an important role in shaping the characteristics of a person.

Behavioural factor: Humans act according to their habitual conducts. When human do things repeatedly over and over again these actions become a habit and are stored in the subconscious minds. Many claimed that good practice security behaviour can enhance employees experience (Munteanu and Fotache, 2015; Safa *et al*., 2015) with regards to the information safety. ISC research found out that security behaviour such as skills (Alfawaz *et al*., 2010; Coventry *et al*., 2014) and self-efficacy (Bozic, 2012; Safa *et al*., 2015, 2016; Vance *et al*., 2012) has an impact towards the security culture of the organisation (Alfawaz *et al*., 2010; Connolly *et al*., 2015; Van Niekerk and Von Solms, 2010). Good security behaviour will result in security compliance thus reduce security breaches. In long term this good behaviour will become norms which exhibit security compliance culture of the organisation.

Environmental factor: Topa and Karyda (2015) and Alfawaz *et al*. (2010) argued that among others, environmental factors that influence the security behaviour of people are still yet to be explored. In reality, human behaviour is very much influenced with the surrounding environment. As an individual, people tendto adapt themselves to the particular situation for the fact that they are unable to change the environment alone. The way the employees behave with regards to security becomes a social norm when the particular conducts seem acceptable by other colleagues and being followed by others (Bozic, 2012). AlHogail (2015) argued that the external environment such as government initiatives, regulation and standard and national culture give impacts towards the security culture of the organisation.

Organisational culture: In order to gain a better insight of security culture in the organisation, research must take into account the cultural values that give impact to the information security compliance behaviour in the organisation. Previous studies proved that organisational culture has an impact to the security culure of the organisation (AlHogail, 2015; Connolly *et al*., 2015; Van Niekerk and Von Solms, 2010). Alnatheer (2015) argued that the organisational culture play an important role to the creation of security culture as employee's behaviour is depending on the cultural values of the organisation. A more rigid culture for instance, emphasizes that rules and regulations must be adhered by all employees whereas a more open culture welcomes ideas and suggestions. This study, employs Wallach (1983) to see if the certain tyes of management style give impact to the governance and management of information seurity in the organisation. WCI has been widely used by scholars of various domains like management, economics and businesses to measure the leadership capability, organisational commitment and customer satisfaction. Wallach (1983) proposed that there are three primary sorts of authoritative societies (i.e., bureaucratic, supportive and innovative). Since, people bring their own qualities, state of mind and convictions to the working environment, their levels of duty to the association may contrast. Da Veiga and Eloff (2010) argued that a bureaucratic organisation will implement a tight and rigid security control to ensure information is safe guarded from being breached. This means that all employees are subject to the security measures including penalty and punishment for any misbehaviours. On the contrary, Connolly *et al*. (2015) debated that information security misbehaviour often occurs in the organisation that discourage employees to implement new ideas and has a clear boundaries of employee-management relationship. By adapting the WCI, this would help clarify these contradictions.

Table 1: Mechanisms of information security governance

Variables/Mechanism	Factors
Structural	Security accountability and responsibility. Decision making initiatives to address and improve security, e.g., task-force, supervision, liaison (Koh *et al*., 2005; Peterson *et al*., 2000; Flores *et al*., 2014; Sulaiman and Jamil, 2014)
Functional	Communication flow system of decision making. Define formal processes for risk analysis, security design, identity and access management, incident management and business continuity (Koh *et al*., 2005; Patnayakuni, 2014; Peterson *et al*., 2000; Flores *et al*., 2014)
Relational	Active participation of key-stakeholders in decision making. Trust environment with shared responsibility for information security shared responsibility for design of policies and compliance (Peterson *et al*., 2000; Koh *et al*., 2005; Patnayakuni, 2014; Flores *et al*., 2014)

Information security governance and management: Security governance must be inclusive to the corporate governance of the organisation (Kooper *et al*., 2011). Security governance is crucial to handle information security related issues (Posthumus and Von Solms, 2004) to make decision with regards to the establishment of standards and principles and alignment with business direction as well as investment priority (Koh *et al*., 2005). Research exposes that security governance has an impact to inculcating good security behaviour of the employees as found out by Koh *et al*. (2005), Patnayakuni (2014) and Flores *et al*. (2014). Our security, governance factor is adapted by Koh *et al*. (2005) and Flores *et al*. (2014) as depicted at Table 1.

The management of information security in the organisation is crucial in deterring information security breaches caused by the insiders. Research shows that the deterrence mechanisms have impact upon inculcating good security behaviour among the staff in the organisation (Connolly *et al*., 2015; D'Arcy and Hovav, 2009). In implementing the security control, top management participationis crucial to ensure that employee behaviour is compliance with the security policy of the organisation (Alnatheer, 2015; Alnatheer and Nelson, 2009; Hu *et al*., 2012; Soomro *et al*., 2016).

It is important that employees are aware of the establishment of the security policy and procedure so that they can adhere (Alnatheer, 2015; Bozic, 2012; Safa *et al*., 2015; Van Niekerk and Von Solms, 2010). Security compliance can be achieved if the employees obtain sufficient training and education with regards to the vulnerabilities, threats and attacks. Social engineering like scam and phishing are among the external culprits which can turn employees into unintentional insider's threat if the employees are not aware enough and well trained in recognising such attack. An organisation must also establish the risks analysis and managementto ensure that the risks can be minimised as low as possible (Alnatheer, 2015; Munteanu and Fotache, 2015; Williams, 2008). D'Arcy *et al*. (2009) found out that physical monitoring is effective in deterring security breaches.

MATERIALS AND METHODS

The study which is exploratory in nature, combines both qualitative and quantitative methods. The pilot study follows an approach suggested by Da Veiga and Eloff (2010). Prior to conducting a pilot study, a set of questionnaire survey has been developed which consists of 149 questions covering all identified factors. The questions were adapted from previous researches such as Siponen *et al*. (2014), Allen (2011), Parsons *et al*. (2014), D'Arcy *et al*. (2009), Safa *et al*. (2016) and Flores *et al*. (2014) and rephrased where possible to suit with the objective of the study. We also developed some of our own questions to complete the questionnaire. The questionnaire uses a 5-Likert scales ranging from 1 for totally disagree/relevant to 5 for totally agree/relevant depending on the questions. To ensure thaat participants are SaaS users, we provide screening questions towards the usage of SaaS applications such as email, social media, cloud storage and some other online applications.

RESULTS AND DISCUSSION

To achieve the objective, 30 IT professionals have been purposely selected to participate in the pilot survey. All of the participants passed our secreening questions to which the degree of the frequency ranging from very limited to extensive usage of SaaS applications. Based on their profile, 70% of the respondents are female staff in the organisation, 57% of them are master and Ph.D holders and 57% of them have more than 15 years working experience. Details of profile is as at Table 2. Out of 30 of them, 10 have been called to further comment on the dimensions and items of the survey. Based on the comments and suggestions from the experts, initial items have been reduced from 149 items to 132 after opting out the redundant questions. The data was analysed using cronbach alpha and composite reliability and the results are as at Table 3.

Based on the result as at Table 3, the Cronbach's alpha and composite reliability for all of the items are above than 0.7. These indicate that the constructs are having internal consistency and reliable (Cohen *et al*., 2013; Nunnally, 1970). The conceptual framework is as shown at Fig. 1.

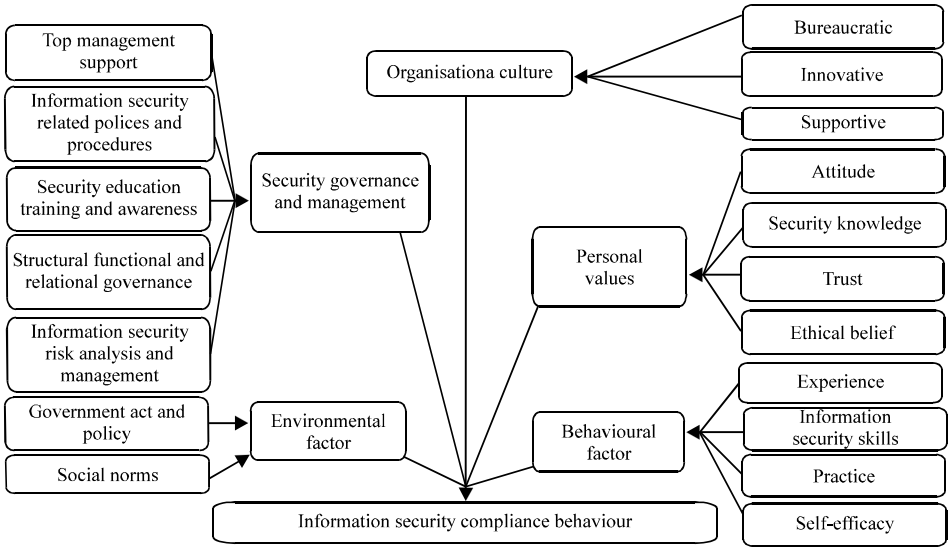

Fig. 1: Conceptual framework

Table 2: Profile of respondents

Variables	Percentage (%)
Gender	
Male	23
Female	77
Qualification	
PhD	31
Master	33
Degree	36
Experience (years)	
<10	7
10-15	36
>15	57

Table 3: Analysis of items

Dimensions	Constructs	Composite reliability	Cronbach's alpha
Organisational culture	C bureaucratic	0.960	0.952
	C supportive	0.969	0.963
	C innovative	0.932	0.923
Behavioural factor	B experience	0.960	0.944
	B practice	0.891	0.863
	B self efficacy	0.970	0.954
	B skills	0.885	0.744
Pesonal values	PC attitude	0.870	0.766
	PC ethics	0.941	0.922
	PC security knowledge	0.880	0.844
	PC trust	0.973	0.963
Environmental factor	Egov act policy	0.914	0.866
	E social norms	0.929	0.902
Infosec governance and management	GMP oli Proc	0.984	0.982
	GMR isk Mgt	0.972	0.964
	GMPhy sec monitor	0.984	0.982
	GMSETA Prg	0.987	0.984
	GMStRl Gov	0.981	0.977

CONCLUSION

The aim of this study is to develop a framework of an information security compliance behaviour. Drawing on social cognitive theory and organisation theory, the integrated soci-organisational factors influencing the security compliance behaviour in the organisation were identified based on the current literature. There are 5 main factors identified; personal characteristics, behaviour, environment, organisational culture as well as information security governance and management. Reliability analysis was done for the data obtained from the pilot study. The analysis shows that all of constructs analysed have Cronbach's alpha >0.7 which indicates significance and reliability of questionnaire. This study, identified significant socio-organisational factors which give impact to the security behaviour of the employees in the organisation, hence the development of the conceptual model.

SUGGESTIONS

Our future research will be testing the conceptual model by conducting a survey to the employees from both public and private sectors. The data will then be analysed using PLS-SEM modeling technique. We plan to complete the research with a case study and interview of selected experts to support our quantitative result.

ACKNOWLEDGEMENTS

We acknowledge the financial support from the Ministry of Higher Education Malaysia, the Universiti Sains Islam Malaysia as well as Universiti Teknikal Malaysia Melaka for their assistance in this research.

REFERENCES

Abdul Hamid, H. and M.M. Yusof, 2015. State-of-the-art of cloud computing adoption in Malaysia: A review. J. Teknologi, 77: 131-136.

Al-Hamar, M., R. Dawson and L. Guan, 2010. A culture of trust threatens security and privacy in Qatar. Proceedings of the 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), June 29-July 1, 2010, IEEE, Bradford, UK, ISBN:978-1-4244-7547-6, pp: 991-995.

AlHogail, A., 2015. Design and validation of information security culture framework. Comput. Hum. Behav., 49: 567-575.

Alfawaz, S., K. Nelson and K. Mohannak, 2010. Information security culture: A behaviour compliance conceptual framework. Proceedings of the 8th Australasian Conference on Information Security Vol. 105, January 1, 2010, Australian Computer Society, Brisbane, Australia, ISBN:978-1-920682-86-6, pp: 47-55.

Allen, S., 2011. The ten commandments of computer ethics. Computer Ethics Institute, Washington, D.C., USA. http://cpsr.org/issues/ethics/cei/

Alnatheer, M. and K. Nelson, 2009. A proposed framework for understanding information security culture and practices in the Saudi context. Proceedings of the 7th Australian Information Security Management Conference, December 1-3, 2009, Perth, Western Australia, pp: 6-17.

Alnatheer, M.A., 2015. Information security culture critical success factors. Proceedings of the 12th International Conference on Information Technology-New Generations, April 13-15, 2015, Las Vegas, NV., pp: 731-735.

Bandura, A., 1989. Social cognitive theory. Ann. Child Dev., 6: 1-60.

Bozic, G., 2012. The role of a stress model in the development of information security culture. Proceedings of the 35th International Convention on MIPRO, May 21-258, 2012, IEEE, Opatija, Croatia, ISBN:978-1-4673-2577-6, pp: 1555-1559.

Castro, D., 2013. How much will PRISM cost the US cloud computing industry?. Inf. Technol. Innov. Found., 2013: 1-9.

Cohen, J., P. Cohen, S.G. West and L. Aiken, 2013. Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences. 3rd Edn., Lawrence Erlbaum Associates Inc, New Jersey, USA., ISBN:0-8058-2223-2,.

Colella, A., A. Castiglione and D.A. Santis, 2014. The role of trust and co-partnership in the societal digital security culture approach. Proceedings of the 2014 International Conference on Intelligent Networking and Collaborative Systems (INCoS), September 10-12, 2014, IEEE, Salerno, Italy, ISBN:978-1-4799-6388-1, pp: 350-355.

Connolly, L. and M. Lang, 2013. Information systems security: The role of cultural aspects in organizational settings. Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy, December 14, 2013, National University of Ireland, Milano, Italy, pp: 1-16.

Connolly, L., M. Lang and J.D. Tygar, 2015. Investigation of employee security behaviour: A grounded theory approach. Proceedings of the IFIP International Conference on Information Security, May 26-28, 2015, Springer, Berlin, Germany, pp: 283-296.

Coventry, L., P. Briggs, J. Blythe and M. Tran, 2014. Using behavioural insights to improve the public's use of cyber security best practices improve the public's use of cyber. Government Office for Science, UK.

D'Arcy, J., A. Hovav and D. Galletta, 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Inf. Syst. Res., 20: 79-98.

Da-Veiga, A. and J.H. Eloff, 2010. A framework and assessment instrument for information security culture. Comput. Secur., 29: 196-207.

Donaldson, L., 1985. In Defence of Organisation Theory: A Reply to the Critics. Vol. 9, Cambridge University Press, Cambridge, UK., Pages: 193.

D'Arcy, J. and A. Hovav, 2009. Does one size fit all? Examining the differential effects of IS security countermeasures. J. Bus. Ethics, 89: 59-71.

Flores, W.R., E. Antonsen and M. Ekstedt, 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Comput. Secur., 43: 90-110.

Gonzalez, N., C. Miers, F. Redigolo, M. Simplicio and T. Carvalho *et al*., 2012. A quantitative analysis of current security concerns and solutions for cloud computing. J. Cloud Comput. Adv. Syst. Appl., 1: 1-18.

Hamid, A.H. and M.M. Yusof, 2016. Conceptualizing global cloud landscape: A review of adoption issues and challenges. Res. J. Appl. Sci., 11: 333-339.

Herath, T. and H.R. Rao, 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst., 47: 154-165.

Hu, Q., T. Dinev, P. Hart and D. Cooke, 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decis. Sci., 43: 615-660.

Kayworth, T. and D. Whitten, 2012. Effective information security requires a balance of social and technology factors. Mis Q. Executive, 9: 163-175.

Koh, K., A.B. Ruighaver, S.B. Maynard and A. Ahmad, 2005. Security governance: Its impact on security culture. Proceedings of the 3rd Conference on Australian Information Security Management (AISM-2005), September 30, 2005, Edith Cowan University, Western Australia, pp: 1-12.

Kooper, M.N., R. Maes and E.R. Lindgreen, 2011. On the governance of information: Introducing a new concept of governance to support the management of information. Intl. J. Inf. Manage., 31: 195-200.

Miller, A., R. Horne and C. Potter, 2015. Information security breaches survey. Department for Business Innovation & Skills, London.

Munteanu, A.B. and D. Fotache, 2015. Enablers of information security culture. Procedia Econ. Finance, 20: 414-422.

Nunnally, J.C. Jr., 1970. Introduction to Psychological Measurement. McGraw-Hill, New York, USA., Pages: 572.

Parsons, K., A. McCormac, M. Butavicius, M. Pattinson and C. Jerram, 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput. Secur., 42: 165-176.

Patnayakuni, R., 2014. Information security in value chains: A governance perspective. Proceedings of the 20th Americas Conference on Information Systems, August 7-9, 2014, Carnegie Mellon University, Pittsburgh, Pennsylvania, pp: 1-10.

Peterson, R.R., R. O'Callaghan and P. Ribbers, 2000. Information technology governance by design: Investigating hybrid configurations and integration mechanisms. Proceedings of the 21st International Conference on Information Systems, December 6-8, 2000, Association for Information Systems, Atlanta, Georgia, USA., pp: 435-452.

Posthumus, S. and R. Von Solms, 2004. A framework for the governance of information security. Comput. Secur., 23: 638-646.

Safa, N.S., M. Sookhak, R.V. Solms, S. Furnell and N.A. Ghani *et al*., 2015. Information security conscious care behaviour formation in organizations. Comput. Secur., 53: 65-78.

Safa, N.S., R. Von Solms and S. Furnell, 2016. Information security policy compliance model in organizations. Comput. Secur., 56: 70-82.

Siponen, M., M.A. Mahmood and S. Pahnila, 2014. Employees' adherence to information security policies: An exploratory field study. Inf. Manage., 51: 217-224.

Soomro, Z.A., M.H. Shah and J. Ahmed, 2016. Information security management needs more holistic approach: A literature review. Intl. J. Inf. Manage., 36: 215-225.

Sulaiman, H. and N. Jamil, 2014. Information security governance model to enhance zakat information management in Malaysian zakat institutions. Proceedings of the International Conference on Information Technology and Multimedia (ICIMU), November 18-20, 2014, IEEE, Putrajaya, Malaysia, ISBN:978-1-4799-5424-7, pp: 200-205.

Topa, I. and M. Karyda, 2015. Identifying factors that influence employees' security behavior for enhancing ISP compliance. Proceedings of the 12th International Conference on Trust and Privacy in Digital Business, September 1-2, 2015, Springer, Valencia, Spain, pp: 169-179.

Van Niekerk, J.F. and R. Von Solms, 2010. Information security culture: A management perspective. Comput. Secur., 29: 476-486.

Vance, A., M. Siponen and S. Pahnila, 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. Inform. Manage., 49: 190-198.

Wallach, E.J., 1983. Individuals and organizations: The cultural match. Train. Dev. J., 37: 28-36.

Williams, P.A., 2008. When trust defies common security sense. Health Inf. J., 14: 211-221.

Zakaria, O., 2006. Internalisation of information security culture amongst employees through basic security knowledge. Proceedings of the IFIP TC-11 21st International Information Security Conference, May 22-24, 2006, Karlstad, Sweden, pp: 437-441.