Information Security Awareness: An Application of Psychological Factors – A Study in Malaysia

Ong Lean-Ping and Chong Chien-Fatt
Southern Cross Business School, Southern Cross University, Australia

Abstract - Current technology advancement promotes borderless environment among individuals, organisations, global industries or public per se. It is akin to having a home but a physical house that is not visible. Looking at the present cybercrime trends, it cannot be disputed that information security is a key matter to observe in the rapid advancement of technology. Information security can be achieved through not only technological and procedural aspects but also the people aspect of information security. An examination of individual's self awareness of information security based on identified key computing areas is carried out through this study. This study aims to provide evidence to organisation(s) in identifying individuals who can be effective defenders to man critical systems and be change agents / ambassadors to cultivate a more security aware community.

Index Terms – Information security awareness, self awareness, five factors model (FFM), theory of planned behavior.

1. Introduction

The revolutionary growth of technology advancement encourages everyone, be it an individual, an organisation, government, a global industry player or community at large, to tap on the convenience, flexibility and ease-of-use features. Borderless environment promoted by technology has enabled information to be shared and transferred at a click on the keyboard or a touch on the monitor screen.

A lay computer user can gain access to information via the Internet at any hour of the day. Organisations and government can easily communicate their missions and directives across their domains with the help of reliable network systems. Community at large can ride on this advanced information technology to share and build up a network of common interests via social networks such as blogs, Facebook, Flicker, LinkedIn, MySpace, Twitter and YouTube.

However, all the convenience, flexibility and ease-of-use features of technology do come with risks. The risks can be in terms of data losses, financial losses, reputation risks, intellectual property or legislation risks.

2. Background

Information security is made up of technology, process and people elements. Technological aspects of information security can be addressed by the implementation or introduction of latest security software, hardware, firewall, encryption methodology, network protection scheme or regular penetration test to system. The procedural aspects of information security can be introduced or enforced through compliance to policies, regulatory requirements, checklists, standards or security certification process. On the other hand, people aspect of information security is very subjective. The current reviewed literatures indicated that there was a lack of a comprehensive review on information security from people aspect [1, 2].

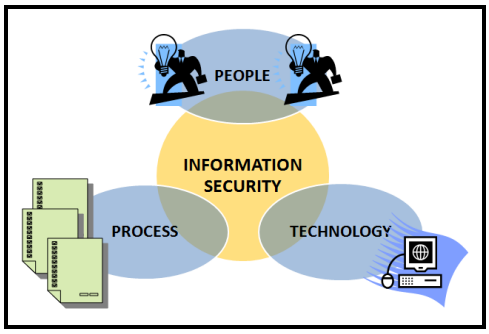

Fig. 1 Aspects on Information Security

A few researchers [3-5] highlighted the notion that information security should be addressed from the people aspect as well and not solely be confined to procedural and technological aspects per se. One of the major fallouts of information security management is the lack of information security awareness among computer users [6-7]. Even though an individual's self awareness of information security is critical, it has been largely ignored as attested by Gehringer [8], Hayashi and Hong [9] and, Thomson and von Solms [10].

There were attempts made to analyse the people aspect of information security awareness from a conceptual view. However, most of these reviewed literatures [11-16] do not provide supporting theoretical backgrounds to the analyses. Most of existing literatures reviewed [17-22] are from organisations' perspectives which dealt with their internal compliance requirements. Therefore, this study will restrict its application and discussion to the people aspect of information security awareness i.e. an individual's self awareness of information security which is the obvious gap of the current situation.

As a matter of fact, the nature of this study has not been explored in the Malaysia context before. It is also the researcher's first attempt to "generalize" this concept through this study although it is done in Malaysia. Therefore, the results of this study will provide an insight and better understanding of individual's self awareness of information security in view of the alarming trend of exposure and risks brought by technology advancement in Malaysia.

Public policy makers and legislators can refer to the study for information to assist in the development of awareness and

training materials for their targeted audience. This can be incorporated into the National Strategy for Cyber Security Acculturation and Capacity Building Program (NSACP) implementation monitored by CyberSecurity Malaysia (CSM) agency under Malaysia's Ministry of Science, Technology and Innovation (MOSTI) [23].

3. Proposed Methodology

The broad problem is usually presented as an initiator to a research / study or by a management question [24, 25]. Following the gap presented, the problem identified for this study is:

'What people aspect can be associated with an individual's self awareness of information security?'

Morin's self awareness model [26] has described both public self-information and private self-information of an individual as contributors to an individual's self awareness on any particular matter or interest. Morin defined private self-information as a kind of conceptual or abstract information of self-aspects in relation to self awareness while public self-information is a kind of perception or visible information of self-aspects like physical characteristics and behaviors [26].

Among the elements of private self-information, the popularity of personality traits among academicians, corporate figures and the general community at large cannot be denied [27]. These traits are also easily understood and commonly researched based on the extensive literature written about it [28-29]. On the other hand, behavior has been assumed by many researchers [30-35] as a key factor in mitigating information security exposure. With these evidences, this study will be restricted to personality traits and behaviour in ascertaining an individual's self awareness of information security. However, this does not mean that the other elements mentioned in Morin's self awareness model are ignored but will essentially be recommended for future study.

A. Personality Traits - Five Factors Model (FFM)

The FFM consists of **E**xtraversion, **A**greeableness, **C**onscientiousness, **N**euroticism and **O**penness factors. John [36] coined the first letter of the above mentioned factors to form the anagram **O.C.E.A.N.** For the purpose of this study, the following conceptual definitions [37] will be referred to.

There are two salient merits for choosing the FFM over other factors such as Myers-Briggs Type Indicator® (MBTI). One of the merits is these five factors demonstrated a high level of stability over a long period across many cultures [27] [38-39]. Secondly, the FFM also provides generalisability in its systematic methodology and approach to personality [40-41]. Therefore, the adoption of FFM for this study is suitable as its features permit use of the model across many cultures and languages of any country globally and across many disciplines, including those in IT and non-IT related fields.

TABLE I Five Factors' Definition

FACTOR	DEFINITION
Openness	The breadth, depth, originality and complexity of an individual's mental and experiential life
Conscientiousness	Socially prescribed impulse control that facilitates task and goal directed behavior, such as thinking before acting, delaying gratification, following norms and rules, and planning, organising and prioritizing tasks
Extraversion	Implies an energetic approach toward the social and material world and includes traits such as sociability, activity, assertiveness and positive emotionality.
Agreeableness	Contrasts a pro-social and communal orientation towards others with antagonism and includes traits such as altruism, tender-mindedness, trust and modesty
Neuroticism	Contrasts emotional stability and even-temperedness with negative emotionality, such as feeling anxious, nervous, sad and tense

B. Behavior – Theory of Planned Behavior

There are three key theories of behaviour widely promoted or considered by many scholars in relation to information security matters [34][42]. They are Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB).

Even though both the TRA and TPB provide useful frameworks for predicting the individual's intention to actual behaviour in a natural context [43-44], several researchers have suggested that TPB is a better predictive model as compared to TRA [45-50]. In order to have a better understanding of what influences the adoption and acceptance of the different information technology contexts, Benbasat and Barki [51] have suggested that researchers make reference to TPB to enable more useful and practical recommendations.

It is also interesting to note that several studies [17], [52-53] have adopted TPB in their research approach on predicting the positioning of information security awareness from the perspectives of an individual's behavior. Hence it is important to consider TPB to be more applicable for this intended study.

C. Key Computing Areas of Interest

The security threats currently facing the world have been categorised into four types in a white paper published by GFI [54]. The types are attacks on physical systems, authentication and privilege attacks, malicious internet content and denial of services. In view of the limited time allocated for this study, only one key computing area from each category will be examined in the context of this study's scope.

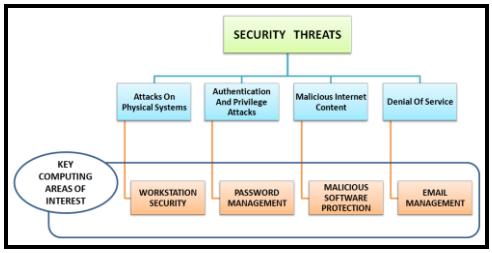

Fig. 2 Security Threats Map and Key Computing Areas of Interest

The areas of interest are Workstation Security, Password Management, Malicious Software Protection and Email Management which mapped to the current identified categories of security threats.

4. Development

With reference to the problem and discussions presented above, a theoretical framework has been conceptualised for this study. The identified independent variables range from an individual's planned behaviour on the proposed key computing areas and individual personality while the dependent variable identified is individual self awareness of information security.

A survey was designed with reference to planned behavior on key computing areas, personality traits and level of self-awareness questionnaires developed by Rahim, Cheo and Cheong [53], Goldberg [55] and Neisser [56] respectively.

5. Participants

Initially, 14 tertiary institutions in Malaysia were approached for this study. However, only 11 of the tertiary institutions expressed interest to participate (a response rate of 78.6 percent). A total of 1250 questionnaires were distributed to the 11 identified tertiary institutions. Thereafter, 606 questionnaires (a response rate of 48.5 percent) were completed and returned to the researcher. The overall number of usable questionnaires upon screening process of the 606 returned questionnaires was 503 (an acceptance rate of 83 percent).

6. Conclusion

From the academic viewpoint and journals publication, there was a lack of a comprehensive review on information security awareness from people element [1]. This is further stressed by Puhakainen [2] that there is a clear need of academic study in information security field which has been perceived to lean towards procedural and technological concern. Despite aggressive promotion and campaign by organisations and government bodies around the world, the level of awareness among computer or internet users in general on information security is still low. This fact in Malaysia context is acknowledged by CyberSecurity Malaysia CEO, Lt-Col (R) Prof Datuk Husin Jazri [57].

The analysis of the data collected for this study is still in progress. Although there were no statistical results to be presented here, the researcher hopes that this paper provides a multi-dimension assessment of an individual's information security awareness level and be of academic value in near future.

On top of that, if the detailed analysis reveals that the multi-dimension assessment is a reliable indicator, then it may be possible to provide evidence to organisation(s) in identifying individuals that can be an effective defender profile to man high risk IT infrastructure. Effective change agent / ambassador to cultivate a more security aware environment and community can be identified as well based on the proposed assessment.

Acknowledgment

The first author would like to thank Dr. Chong Chien-Fatt for his supervisory role throughout the study and all of the participants from 11 tertiary institutions in Malaysia who filled out the study's questionnaires. Thanks also to Dr. Michelle Wallace (Associate Professor and Director, Doctor of Business Administration at Southern Cross University) for her guidance and Dr. Daniel D. Reidpath (Professor of Population Health at Monash University Malaysia and Director, South East Asia Community Observatory) for his assistance with initial statistical analysis.

References

[1] Iivari, J & Hirschheim, R 1996, 'Analyzing information systems development: A comparison and analysis of eight development approaches', *Information Systems*, vol. 21, no. 7, pp. 551-575.

[2] Puhakainen, P 2006, 'A design theory for information security awareness', *Acta Universitatis Ouluensis A463*, University of Oulu, Finland.

[3] Dhillon, G & Torkzadeh 2006, 'Value focused assessment of information system security in organizations', *Information Systems Journal*, vol. 16, pp. 293–314.

[4] Salahuddin, A, Karen, N & Kavoos, M 2010, 'Information security culture: A behavior compliance conceptual framework', *Australasian Information Security Conference (AISC)*, Brisbane, Australia.

[5] Siponen, MT & Oinas-Kukkonen, H 2007, 'A review of information security issues and respective research contributions'. *ACM SIGMIS Database*, vol. 38, no. 1, pp. 60-80.

[6] von Solms, B & von Solms, R 2004, 'The 10 deadly sins of information security management', *Computers & Security*, vol. 23, pp. 371-376.

[7] Wilson, M & Hash, J 2003, 'Computer security - Building an information technology security awareness and training program', *National Institute of Standards and Technology*, NIST Special Publication 800-50.

[8] Gehringer, EF 2002, 'Choosing passwords: Security and human factors', *International Symposium on Technology and Society*, ISTAS'02, pp. 369-373.

[9] Hayashi, E & Hong, JI 2011, *'A diary study of password usage in daily life', CHI 2011, May, Vancouver, BC, Canada.*

[10] Thomson, ME & von Solms, R 1998, 'Information security awareness: Educating your users effectively', *Information Management & Computer Security*, MCB University Press Limited, vol. 6, no. 4, pp. 167-173.

[11] Forcht, KA, Pierson, JK & Bauman BM 1988, 'Developing awareness of computer ethics', *Association for Computing Machinery*, pp. 142-143.

[12] Kajava, J & Varonen, R 2002, 'IT and the human body and mind in the information security perspective', *European Intensive Programme on Information and Communication Technologies Security*, pp.1-10.

[13] Shamsul KWF, Mohd Nabil Z, Mohd Sazili S, Juwahir A & Muhammad Khairulnizam Z 2012, 'Information security awareness amongst academic librarians', *Journal of Applied Sciences Research*, vol. 8, no. 3, pp. 1723-1735.

[14] Shaw, E, Ruby, K & Post, J 1998, 'The insider threat to information systems: The psychology of the dangerous insider', *Security Awareness Bulletin*, No. 2-98.

[15] Spurling, P 1995, 'Promoting security awareness and commitment', *Information Management & Computer Security*, MCB University Press Limited, vol. 3, no. 2, pp. 20-26.

[16] Stacey, TR 1996, 'The information security program maturity grid', *Information System Security*, vol. 5, no. 2, pp. 22-33.

[17] Banerjee, D, Cronan, TP & Jones, TW 1998, 'Modeling IT ethics: A study in situational ethics', *MIS Quarterly*, March 1998, pp. 31-60.

[18] Kruger, HA & Kearney WD 2006, 'A prototype for assessing information security', *Computer & Security*, Elsevier Ltd., vol. 25, pp. 289-296.

[19] Risvold, MO 2010, 'Organizational issues related to information security behavior', Lulea University of Technology.
[20] Stephanou, AT & Dagada, R 2008, 'The impact of information security awareness training on information security behavior: The case for further research', University of the Witwatersrand.
[21] Takemura, T 2011, 'Statistical analysis on relation between workers information security awareness and the behaviors in Japan', *Journal of Management Policy and Practice*, vol. 12, no. 3, pp. 27-36.
[22] Takemura, T & Umino, A 2009, 'A quantitative study on Japanese internet users' awareness to information security: Necessity and importance of education and policy', *World Academy of Science, Engineering and Technology*, vol. 60, pp. 638-644.
[23] Yunos, Z 2012, 'Collaborative model toward achieving security and safety in the cyber environment', *ASEAN Regional Forum Seminar on Confidence Building Measures in Cyber Space*, Seoul, Korea, CyberSecurity Malaysia, MOSTI, 11-12 September 2012.
[24] Berg, BL 2004, *Designing Qualitative Research*, Qualitative Research Methods, Pearson, Boston.
[25] Cooper, DR & Schindler, PS 2003, *Business Research Method*, 8th edn, McGraw Hill, Irwin.
[26] Morin, A 2006, 'Levels of consciousness and self-awareness: A comparison and integration of various neurocognitive views', *Consciousness and Cognition*, vol. 15, pp. 358–371.
[27] Schultz, DP & Schultz, SE 2009, *Theories of Personality*, 9th edn, Wadsworth, Cengage Learning, USA.
[28] Cloninger, S 2009, *Theories of Personality: Understanding Persons*, 5th edn, Pearson Education Inc., New Jersey.
[29] John, OP, Naumann, LP & Soto, CJ 2008, 'Paradigm shift to the integrative Big Five trait taxonomy', *Handbook of Personality: Theory and Research* (pp. 114-158), eds. OP, John, RW, Robins & LA, Pervin, 3rd edn, The Guilford Press, New York.
[30] Chen, CC, Shaw, RS & Yang, SC 2006, 'Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system', *Information Technology, Learning and Performance Journal*, vol. 24, no. 1, pp. 1-14.
[31] Hentea, M 2005, 'A perspective on achieving information security awareness', *Informing Science and IT Education Conference Proceedings*, pp. 169-178, Flagstaff, Arizona, USA.
[32] Kajava, J & Siponen, MT 1997, 'Effectively implemented information security awareness - An example from University Environment. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1)'. *13th International Conference on Information Security: Information Security Management - The Future*, 13th May 1997, Copenhagen, Denmark.
[33] Kajava, J & Siponen, MT 2002, 'IT security awareness - Issues of industry', *European Intensive Programme on Information and Communication Technologies Security*, IPICS, 3rd Winter School, Oulu, Finland.
[34] Siponen, MT 2000, 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security*, vol. 8, no. 1, pp. 31-41.
[35] Tsohou, A, Koklakis, S, Karyda, M & Kiountouzis, E 2008, 'Investigating information security awareness: Research and practice gaps', *Information Security Journal: A Global Perspective*, vol. 17, pp.207-227, Taylor & Francis Group, LLC.
[36] John, OP 1990, 'The "Big Five" factor taxonomy: Dimensions of personality in the natural language and in questionnaires', *Handbook of Personality: Theory and Research* (pp. 66-100), The Guilford Press, New York.
[37] John, OP & Srivastava, S 1999, 'The Big-Five trait taxonomy: History, measurement, and theoretical perspectives', University of California.
[38] Costa, PT Jr & McCrae, RR 1988, 'Personality in adulthood: A six-year longitudinal study of self-reports and spouse ratings on the NEO personality inventory', *Journal of Personality and Social Psychology*, vol. 54, pp. 853-863.
[39] McCrae, RR 2000, 'Trait psychology and the revival of personality and cultural studies', *American Behavioral Scientist*, vol. 44, pp. 10-31.
[40] Arthur, W & Grazziano, W 1996, 'The Five-Factor Model, conscientiousness and driving accident involvement', *Journal of Personality*, vol. 64, no. 3, pp. 594-618.
[41] Goldberg, LR 1993, 'The structure of phenotypic personality traits', *American Psychologist*, vol. 48, pp. 26-34.
[42] Ramayah, T & Muhamad, J 2004, 'Technology acceptance: An individual perspective - current and future research in Malaysia', *Review of Business Research*, IABE, vol. 2, no.1, pp. 103-111.
[43] Hale, JL, Householder, BJ & Greene, KL 2003, 'The persuasion handbook: Developments in theory and practice - The theory of reasoned action', Thousand Oaks, CA: Sage, pp. 259-286.
[44] Taylor, S & Todd, P 1995, 'Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions', *International Journal of Research in Marketing*, vol. 12, no. 2, July 1995 , pp. 137-155, Elsevier.
[45] Albarracin, D, Johnson, BT, Fishbein, M & Muellerleile, PA 2001, 'Theories of reasoned action and planned behavior as models of condom use: A meta-analysis', *Psychological Bulletin*, vol. 127, pp. 142-161.
[46] Caron, F, Godin, G, Otis, J & Lambert, LD 2004, 'Evaluation of a theoretically based AIDS/STD peer education program on postponing sexual intercourse and on condom use among adolescents attending high school', *Health Education Research*, vol. 19, no. 2, pp. 185-197.
[47] Godin, G & Kok, G 1996, 'The theory of planned behavior: A review of its applications in health-related behaviors', *American Journal of Health Promotion*, vol. 11, pp. 87-98.
[48] Hagger, MS, Chatzisarantis, NLD & Biddle, SJH 2002, 'A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables'. *Journal of Sport & Exercise Psychology*, vol. 24, pp. 3-32.
[49] Hausenblas, HA, Carron, AV & Mack, DE 1997, 'Application of the theories of reasoned action and planned behavior to exercise behavior: A meta- analysis', *Journal of Sport & Exercise Psychology*, vol. 19, pp. 36-51.
[50] Sheeran, P & Taylor, S 1999, 'Predicting intentions to use condoms: A meta-analysis and comparison of the theories of reasoned action and planned behavior', *Journal of Applied Social Psychology*, vol. 29, pp. 1624-1675.
[51] Benbasat, I & Barki, H 2007, 'Quo vadis, TAM?', *Journal of the Association of Information Systems*, vol. 8, no.4, pp. 211–218, April.
[52] Ng, BY and Rahim, MA 2005, 'A socio-behavioral study of home computer users' intention to practice security', *The Ninth Pacific Asia Conference on Information Systems*, Jul 2005, pp. 234-247.
[53] Rahim, MM, Cheo, A & Cheong, K 2008, 'IT security expert's presentation and attitude changes of end-users towards IT security aware behavior', *19th Australasian Conference on Information Systems*, 3-5 Dec, Christchurch, pp. 780-790.
[54] GFI 2009, Security Threats: A Guide for Small and Medium Businesses, 5 March 2009, White Paper.
[55] Goldberg, LR 1992, 'The development of markers for the Big-Five factor structure', *Psychological Assessment*, vol. 4, no. 1, pp. 26-42.
[56] Neisser, U 1988, 'Five kinds of self-knowledge', *Philosophical Psychology*, vol. 1, no. 1, pp. 35-59, Routledge, UK.
[57] Kumar, A 2011, 'Malaysians need to increase security awareness', *Computerworld Malaysia*, 13 May.