Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME

Jasber Kaur
Faculty of Computer & Mathematical Sciences,
Universiti Teknologi MARA Malaysia,
jasber@tmsk.uitm.edu.my

Norliana Mustafa
Faculty of Computer & Mathematical Sciences,
Universiti Teknologi MARA Malaysia,
vada_adore@yahoo.com

Abstract-*The role and importance of information security policy is gaining its popularity in many large organisations. However, this is not the case for SMEs as developing and adopting information security policy requires a lot of time and resources. Lack of awareness, thus, exposes organisation to significant risk in ensuring security and protection of organisational assets. This paper reports awareness of information security at a SME in Malaysia. The research aims to establish the relationship between knowledge, attitude and behaviour and information security awareness. A survey questionnaire was used to collect data about information security awareness. Partial-least square was used for data analysis. The findings present information security awareness of employees indicating attitude and behaviour found to be significantly influence confidentiality, integrity, and availability (CIA) of business information.*

Keywords-small and medium enterprise; information security; information security awareness

I. INTRODUCTION

All organisations rely heavily on the internet, investing significant resources as means to compete in today's global marketplace [1]. This investments, however exposes organisations to risks and threats that resulted in major losses such as financial, brand and reputation. To protect from this adverse risks and threats, companies often resort to security technologies implemented to protect business information. However, according to Herath and Rao [2] such technologies have been found to be insufficient to ensure security. Security technologies and techniques can be misused and are vulnerable to attacks, therefore losing its usefulness [3]. Thus, end user commitment and behaviour plays profound role in ensuring security and integrity of organisational business assets, information, hardware and networks. Users' responsibilities and behaviour towards the safeguard of organisational assets, business information, computers and network resources cannot be dealt by implementing security technologies.

According to Posthumus and von Solms [4], three major elements of information security encompasses safeguarding information's confidentiality, integrity and availability in alleviating risks and threats through a series of security controls. Whilst, creating and maintaining *security-positive behaviour* to ensure information security is defined as information security awareness [5]. ISF [6] define information security awareness as individual responsibilities of their own individual security responsibilities, understanding the importance of information security that is appropriate to organisation and to act accordingly.

In a recent survey by Australian Chamber of Commerce and Industry (ACCI), revealed that 60% of small businesses suffered security breach in 2012. PricewaterhouseCoopers reported that 76% of small businesses in United Kingdom suffered security breaches which have caused financial losses. Although the importance of information security is essential in protecting organisational assets, developing and enforcing information security requires time and resources, thus presenting challenges to SMEs due to its organisation size. In particular, SMEs are not prepared to adopt information security simply because a documented information security is not required due to its small size [7]; [8]. Nevertheless, it is imperative to know perception of end users to information security adopted and whether they are aware of information security policy implemented in organisation. Thus, the research question is formulated accordingly; *Is there a relationship between knowledge, attitude and behaviour to information security awareness?* The research aims to determine the relationship among knowledge, attitude and behaviour to information security awareness using partial least square.

The structure of this paper is as follows. After introducing the need for information security awareness, the second section will position information security attributes in relation with psychological factors and their hypotheses. Section three describes the data collection procedure at a single case site, and thereafter analysis of the results. And the last section will conclude the findings and discussion on the limitation of this paper.

II. LITERATURE REVIEW AND HYPOTHESES

This section discusses the theoretical foundations for the research. Drawing on literature on information security and social psychology, we seek to establish and test a theoretical model.

Maintaining information security generally focuses on protecting three main aspects of confidentiality, integrity and availability of information [5]; [9]. Confidentiality, integrity and availability (CIA) serves as major and critical attributes for information security management objectives [10]. According to McLeod and Schell [9], confidentiality is referred to as protection of data and information from disclosure to unauthorised person; integrity as providing an accurate representation of the physical reality that data

represents; and availability is about allowing those authorised to have access to data. Therefore an attack is detrimental to organisational asset by affecting its confidentiality, integrity, or availability, henceforth, possibility of business losses.

According to Cox, Connolly and Currall [11], human behaviour is very crucial in ensuring efficient environment for information security and cannot rely entirely on technical solutions. Based from social psychology field, Kruger and Kearney [5] developed a prototype for measuring information security awareness using knowledge, attitude and behaviour (KAB). The underlying theory for KAB is that it seeks to understand the relationship between these three components, suggesting that as knowledge accumulates in a relevant behaviour, say for example in information security, health, education, it will eventually initiate changes in attitude that will gradually initiate the change in behaviour.

Throughout the research, information security awareness is an integrated model encompasses KAB [12]; [13] and components of information security including CIA [12]; [14]; [15]. In KAB, knowledge refers to the focus of what an employee knows; attitude focuses on what an employee think; and behaviour is about what an employee does.

Accordingly, knowledge is based on user knowledge on how to behave in certain condition [12]. The ability to maximise confidentiality, integrity and availability of information, is based on the ability of knowing what these concepts mean [16]. As an example, in order to minimise virus infection from utilisation of internet and email in responsible manner, knowing that scanning all attachment to e-mails and only access trusted sites is able to maximise the confidentiality of data, the concept of using strong password is able to maximise the integrity of data from unauthorised access, and the concept of maximising the information transfer of regular backups to alternative locations is able to maximise the availability of data [17]. Users' who are equipped with proper knowledge has the ability to prevent threats and attacks, thus increases confidentiality, integrity and availability of information [18]. Therefore, it is hypothesised that:

H1a: There is a significant relationship between knowledge and confidentiality.
H1b: There is a significant relationship between knowledge and integrity.
H1c: There is a significant relationship between knowledge and availability.

Attitude refers to users' attitude (how you feel or beliefs) towards possible consequences of such behaviour [12]. User belief to maximising integrity of data, consistency of data can be maintained to minimise unauthorised access [19]. User belief that keeping password a secret and that it should not be written down or given to others will ensure from unauthorised access which then leads to maximising confidentiality of data [5]. Accordingly, user may belief that maximising availability through uninterrupted usage of data is simply making sure that hardware and equipments are available and in working condition [17]. Thus, we hypothesise:

H2a: There is significant relationship between attitude and confidentiality.
H2b: There is significant relationship between attitude and integrity.
H2c: There is significant relationship between attitude and availability.

The notion of behaviour is based on what employee does and relates to actual behaviour [12]. As an example, keeping passwords a secret and assuring that passwords are strong and that it remains as a strong password [16]. Scanning email attachments for viruses is a good partice to prevent loss of data as a result from virus infection which can further compromise integrity of data. Regularly running data backups in other locations prevents disruption of availability of data. Thus, it is hypothesise that:

H3a: There is significant relationship between behaviour and confidentiality.
H3b: There is significant relationship between behaviour and integrity.
H3c: There is significant relationship between behaviour and availability.

Fig. 1 shows the present research theoretical model.

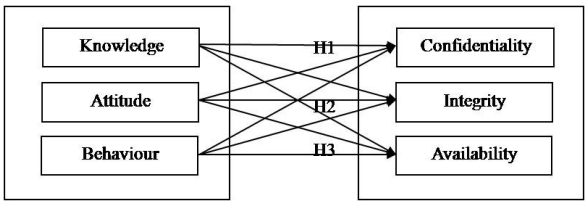

Fig. 1. Research model

III. RESEARCH DESIGN

A. Research Context

The research was conducted with employees as research participants at a small and medium enterprise in Malaysia. The company background chosen is from an aeronautical industry primarily focuses on developing aerospace technologies. A survey questionnaire was used as the instrument.

B. Population and Sampling

The estimated population for the research is 110. Due to the small number in population size, questionnaire was distributed to all respondents in the population.

C. Measures

The instrument was designed to evaluate employees' information security awareness which consists of 31 items. Instrument contained seven point Likert-scale to measure for knowledge, attitude, behaviour, confidentiality, integrity and availability attributes. The scale was refers to 1 as strongly disagree to 7 as strongly agree.

D. Data Analysis

Descriptive analysis and reliability analysis were made using SPSS version 16 for Windows. Path analysis approach was adopted using SmartPLS 2.0 version M3.

IV. RESULTS

A. Descriptive Profile of Sample

Table 1 shows the breakdown of respondents by gender, age and number of years experience in information systems. The analysis is reported in frequency and percentage.

TABLE 1. PROFILE OF RESPONDENTS

Profile of Respondents		Frequency	%
Gender	Male	64	75.3
	Female	21	24.7
Age	21-30	9	10.6
	31-40	20	23.5
	41-50	19	22.4
	Above 50	37	43.5
Number of years experience in IS	1-3	9	10.6
	4-6	15	17.6
	7-9	8	9.4
	10-12	20	23.5
	More than 12	33	38.8
	Total	85	

The table showed that majority of respondents were male (75.3%). The age distribution of respondents showed that majority of respondents belongs into the age group of above 50 years old (43.5%). As the organisation core business involves aerospace technologies, retired employees from related industry are hired due to their skill and experience. Majority of the respondents (38.8%) have more than 13 years of experience in information systems.

B. Descriptive Profile of Measurement Item

Table 2 shows the result of Likert-scale measures. Generally the mean value for knowledge, attitude, behaviour, confidentiality, integrity and availability are well above 5.00. This indicates that the majority agrees with the statements.

TABLE 2. PROFILE OF LIKERT-SCALE MEASURES

Measures	Mean
Knowledge	
1. I have the necessary knowledge to handle information security in my working situation. (K1)	5.74
2. I know what information security is. (K2)	5.56
3. I know what an information security incident is. (K3)	5.48
4. Internet access on the company's system is a corporate resource and should be used for business purposes only. (K4)	6.21
5. Phishing e-mail is the act of stealing users' sensitive and personal information. I am familiar with this threat. (K5)	6.13
Average knowledge score:	5.83
Attitude	
6. My practice in handling sensitive information is appropriate and effective. (A1)	6.46
7. My practice in exercising care when opening a suspicious email is a wise move. (A2)	6.45
8. In my view, using password protected computer is as wise ideas. (A3)	6.67
9. The thought of using antivirus program is appealing to me. (A4)	6.49
10. Using the Firewall system at work is a good idea. (A5)	6.56
Average attitude score:	6.53
Behaviour	
11. I am aware that I should never give my password to somebody else; however, my work is such a nature that I do give my password from time to time to a colleague that I trust. (B1)	5.39
12. I do not open email attachments if the content of the email looks suspicious. (B2)	6.50
13. Before reading an email, I will first check if the subject and the sender make sense. (B3)	6.55
14. I never give my personal information (like home/email address, telephone number, etc.) to unknown websites. (B4)	6.74
15. I never download files (like documents, music, picture, software, etc.) from the Internet if the files are from unknown people. (B5)	6.22
16. I pay attention to anti-virus updates every time I use a computer. (B6)	5.52
Average behaviour score:	6.16
Confidentiality	
17. Your company has well implemented security practices to protect important information from stolen by malicious intrusions (such as break-in, Trojans, and spy-wares). (C1)	6.24
18. Unauthorized employees are prohibited from accessing company's information resources. (C2)	6.74
19. Information security measures are implemented in your company to prevent sensitive information from unauthorized disclosure. (C3)	6.35
20. Logging all access attempts of confidential files is mandatory. (C4)	6.58
21. Physical access control is always no.1 priority. (C5)	6.79
Average confidentiality score:	6.54
Integrity	
22. The database is periodically reconciled and regularly maintained in order to increase the accuracy and reliability of information. (I1)	6.44
23. When acquiring important information from the information sources or business partners, the information will be stored into the company's database. (I2)	6.58
24. Your company has security controls (such as change management procedures) in place to prevent unauthorized information changes (creation, alternation, and deletion). (I3)	6.36
25. Information should be protected or secured from unauthorized use. (I4)	6.81
26. The privacy of employees and customers should be protected. (I5)	6.84
27. Integrity of the information on systems must be maintained. (I6)	6.76
Average integrity score:	6.63
Availability	
28. The probability of information system breakdown and information service disruption in my organization is low. (Av1)	5.92
29. A legitimate user with business needs can access company information at anytime and at any place. (Av2)	6.53
30. The company should have redundancy in hardware to tolerate hardware failure. (Av3)	6.78
31. All servers should be continuously available to their clients. (Av4)	6.76
Average availability score:	6.50

C. Partial Least Square Findings

Partial least square is a predictive modelling technique to detect relationships among constructs. Construct validity is established to ensure reliability and validity of

measures that represent a construct. Several criteria will be assessed such as composite reliability (above 0.6), average variance extracted (AVE) (above 0.5) and discriminant validity must be established [20]. Table 3 summarises reliability and validity for each construct. The table shows that item reliability ranges between 0.523 and 0.927 which showed an acceptable reliability as it is above the estimated range of 0.50 [21]. The composite reliability ranges between 0.89 and 0.93 indicating an acceptable scale. The score is above 0.60, as per recommendation by [22]. Average variance extracted (AVE) shows scale above 0.50 which presents an acceptable construct [23]. Since all reliability and validity test is satisfied, therefore construct validity is established.

TABLE 3. LOADING, CR AND AVE

Construct	Item reliability	Composite reliability	AVE
Knowledge			
K1	0.869		
K2	0.902	0.926	0.718
K3	0.756		
K4	0.750		
K5	0.824		
Attitude			
A1	0.815		
A2	0.843	0.934	0.739
A3	0.812		
A4	0.738		
A5	0.790		
Behaviour			
B1	0.788		
B2	0.831		
B3	0.832	0.895	0.631
B4	0.523		
B5	0.684		
B6	0.796		
Confidentiality			
C1	0.819		
C2	0.628		
C3	0.834	0.890	0.619
C4	0.768		
C5	0.801		
Integrity			
I1	0.782		
I2	0.777	0.921	0.662
I3	0.807		
I4	0.927		
I5	0.893		
Availability			
Av1	0.629		
Av2	0.756	0.892	0.677
Av3	0.847		
Av4	0.770		

The inter-construct correlations were shown in Table 4. The square-root of AVE were higher than correlations, thus supporting discriminant validity.

TABLE 4. INTER-CONSTRUCT CORRELATIONS

	K	A	B	C	I	Av
Knowledge (K)	**0.847**					
Attitude (A)	0.653	**0.860**				
Behaviour (B)	0.774	0.674	**0.795**			
Confidentiality (C)	0.701	0.709	0.791	**0.787**		
Integrity (I)	0.638	0.608	0.669	0.883	**0.814**	
Availability (Av)	0.539	0.697	0.638	0.791	0.810	**0.822**

Fig. 2, shows path results for the research model. The values stated on the path are path coefficient and t-value (in bracket).

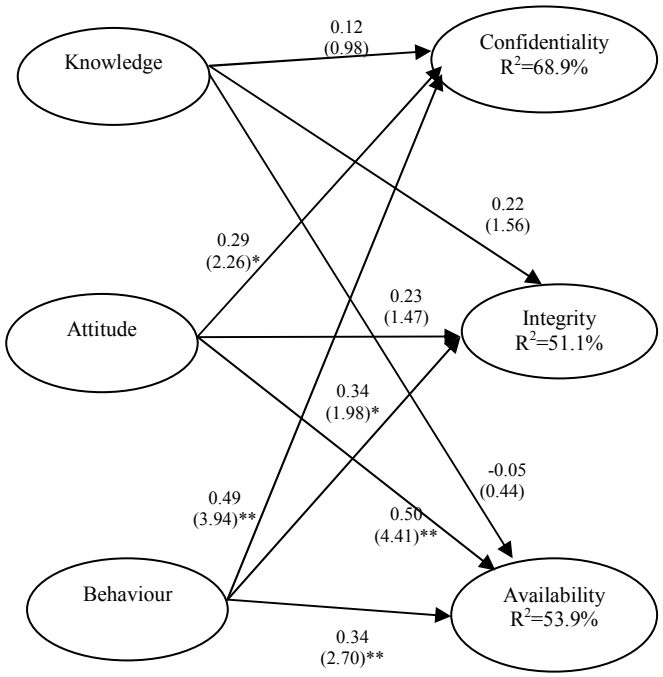

Fig. 2. Path Results

68.9% of the variance in confidentiality can be explained by attitude and behaviour. 51.1% of the variance in integrity can be explained by behaviour. Availability accounts for 53.9% of the variance explained by attitude and behaviour. Out of the original nine hypothesised relationships, five hypotheses found to be significant.

Surprisingly there is no significant relationship between knowledge and confidentiality, integrity and availability. The findings indicate that attitude and behaviour are the determinants of confidentiality, suggesting that employees have necessary attributes of attitude and behaviour in performing measures to ensure confidentiality of information. The findings also show that, only behaviour influence integrity, suggesting that users have the necessary attributes of behaviour to ensure integrity. Our findings also indicate that only attitude and behaviour are the determinants for availability, suggesting that users might have the necessary attributes of attitude

and behaviour while knowledge is not significant to availability.

V. CONCLUSION

This study started with the concern over information security awareness among SMEs. In line with the research objectives, this research has attempted to evaluate information security awareness among employees in a SME. The findings were summarised as follows:

- The findings indicate that there are significance relationship between users' attitude and behaviour with information security awareness. Knowledge showed no significant relationship with information security awareness.
- The findings also indicate that attitude and behaviour had significant relationship to confidentiality suggesting that employees are aware of their responsibilities in maintaining confidentiality of the business information and resources.
- Feedbacks from users indicate that they lack necessary knowledge in handling information security issues, such as phishing email. This could explain the non significance of knowledge construct. Organisation should play a role in educating and improving employees' knowledge in information security.

Cyber Security Malaysia has published Information Security guidelines for Small and Medium Enterprises (SMEs). The guideline indicates important aspects in handling information security and basic principle in executing information security.

The research presents limitation that should be acknowledged. Sample size in this study is limited to one organisation, therefore findings cannot be generalised to all SMEs. Future work should consider replicating the study to other SMEs.

REFERENCES

[1] Tawileh, A., Hilton, J., and McIntosh, S. (2007). Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. Information Security Solutions Europe/SECURE 2007 Conference, Vieweg, 331-339.

[2] Herath, T., and Rao, H. (2007). Encouraging Information Security Behaviour in Organisation: Role of Penalties. Journal of Decision Support System , 154–165.

[3] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 31-41.

[4] Posthumus, S., and von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 638-646.

[5] Kruger, H., and Kearney, W. (2006). A prototype for assessing information security awareness. Computers & Security, 289-296.

[6] Information Security Forum. (2003, March). Retrieved June 19, 2012, from The Standard of Good Practice for Information Security: http://www.netbotz.com/library/Info_Security_Forum_Standard_God_Practices.pdf

[7] Kuusisto, T., and Ilvonen, I. (2003). Information Security Culture in Small and medium size enterprises. Frontiers of e-business research , 431-439.

[8] Doherty, N. F., and Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. Information Resources Management Journal, 20-38.

[9] Mcleod, R., and Schell, J. G. (2008). Management Information Systems. London: Pearson Education.

[10] Ma, Q., Johnston, A. C., and Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. Information Management & Computer Security, 251-270.

[11] Cox, A., Connolly, S., and Currall, J. (2001). Raising information security awareness in the academic setting. VINE , 11-16.

[12] Kruger, H., and Kearney, W. (2008). Consensus ranking – An ICT security awareness case study. Computers & Security , 254–259.

[13] Khan, B., Alghathbar, K. S., Nabi, S. I., and Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management , 10862-10868.

[14] Wang, A. J. (2005). Information Security Models and Metrics. 43rd ACM Southeast Conference, 177-184.

[15] Andress, J. (2011). The basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. MA: Syngress.

[16] Kruger, H., Drevin, L., and Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security , 316-327.

[17] Kruger, H., Drevin, L., and Steyn, T. (2007). Value-focused assessment of ICT security awareness. Computer & Security , 36-43.

[18] Sabeeh, A., and Lashkari, A. H. (2011). Users' Perceptions on Mobile Devices Security Awareness in Malaysia. International Conference for Internet Technology and Secured Transactions, Abu Dhabi: IEEE, 428-435.

[19] Kruger, H., and Kearney, W. (2005). Measuring information security awareness: A West Africa gold mining environment case study. Proceedings of the 2005 ISSA Conference. Johannesburg , 1-10.

[20] Henseler, J., Ringle, C. M., and Sinkovics, R. R. (2009). The Use of Partial Least Squares Path Modeling in International Marketing. *Advances in International Marketing, 20*, 277–319.

[21] Hair, J. F., Black, B., Babin, B., Anderson, R. E., and Tatham, R. L. (1998). Mutivariate Data Analysis. NJ: Prentice-Hall.

[22] Bagozzi, R. P., and Yi, Y. (1988). On the evaluation of structural equation models. Journal of the Academy of Marketing Science , 74–94.

[23] Fornell, C., and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research , 39–50.