asian academic accounting association

Available online at
www.foura.org

ASIAN ACADEMIC ACCOUNTING ASSOCIATION
18th annual conference
22-23 NOVEMBER 2017. BALI, INDONESIA

Does Organisational Culture Affect Dysfunctional Behaviour in Information System Security?

Saiyidi Mat Roni[a], Hadrian Geri Djajadikerta*[a], Terri Trireksani[b]

[a] *School of Business and Law, Edith Cowan University, Australia*
[b] *School of Business and Governance, Murdoch University, Australia*

Abstract

Information system (IS) security incidents occur, in part, because employees undermine security policy. While existing studies suggest organisational culture influences employee behaviour in ways that can comprise IS security, examining organisational culture as a single component, or investigating only one dimension of culture, can put the discipline at harm. This is because organisational culture is a conjugation of multifaceted collective beliefs that materialises in actions and artefacts. Investigating organisational culture at only its higher order level can mask dimensional effects of culture at its lower order factors. This study provides additional insight into the body of knowledge in IS security by examining organisational culture at its higher order and at its dimensions in order to investigate how these dimensions play their roles in the realm of IS security non-compliance and intentional violations.

Keywords: Organisational culture, information system security, dysfunctional behaviour.

1. INTRODUCTION

A multimillion dollar series of hacks of automated teller machines (ATM) in Taiwan (July 2016, estimated loss of USD2.6 million), Thailand (August 2016, estimated loss of USD350,000), and Malaysia (Sep 2014, estimated loss of USD850,000) was mostly enabled by the banks' failure to upgrade to the latest operating system, or to update security patches of ATMs' operating system – Windows XP – which was discontinued by Microsoft in 2007.

Instituting regular software updates has become an increasingly pressing requirement in recent years, as there are approximately five defects for every 1000 lines of code (Mason & Bohm, 2017), which makes any system vulnerable for security breaches. This should have been realised by the banks, and those responsible for information system security should have foreseen the vulnerability residing in their ATMs. Regretfully, the banks remained unresponsive to this security pandemonium until a threat became a theft.

What led the banks, the management, and employees entrusted with ATM security to play down the risk was perplexing to some, and interesting for others to investigate. Their actions or inactions are partly shaped by the organisational culture in which they interact. Organisational culture is known to influence employee behaviour. This is true regardless of whether the behaviour is good or, conversely, merely perceived as good despite being detrimental to the organisation in the long run. This heuristic behavioural model inculcated by the sociology of an organisation prompting the members to fall back on simple behavioural rules rather than a thoughtful decision; and in the case of the ATMs heist – the decision to not do anything.

* Corresponding author. Tel.: +61-8-6304 5353
E-mail: h.djajadikerta@ecu.edu.au

The connotation remains similar in the context of information system (IS), where security incidents in organisations occur partly due to employee actions that undermine existing IS security policy. These behaviours, either volitional or unintentional, fall under the umbrella of dysfunctional behaviour (Djajadikerta, Mat Roni, & Trireksani, 2015; Mat Roni, 2015). In situations where outcomes are priorities, short-cuts and transgressions of IS security policies can be seen as 'allowable' to get the job done, particularly when the transgression is routinized. This is evidenced in studies by D'Arcy and Hovav (2009), D'Arcy and Herath (2011), and Davis and Pesch (2013), which show that an interaction between the employee and the organisational facades has profound effects on the efficacy of control mechanisms.

Despite reports by many studies (e.g. Baker et al., 2011; "KPMG's fraud survey 2009," 2009; Liang, Biros, & Luse, 2016) that point to increasing severity of dysfunctional behaviour originating from within, the organisational approach towards IS security is largely anchored on external threats. Addressing the insider threats to IS by merely focussing on the hard measures, such as passwords and administrator privileges, alone is not sufficient. As the rules prescribe the employees' actions, the interaction between the employees and the organisational facets defines the sociology of the organisation and thus conjugates in part to the effectiveness of IS security. Dang-Pham, Pittayachawan, and Bruno (2017), for example, suggest that a constant interaction between employees can influence oneself to conform to group norms. Therefore, addressing the issue of employee dysfunctional behaviour in the IS environment warrants countermeasures beyond the scope of what technological controls can offer. Effectively implementing such countermeasures requires a thorough understanding of the tenets of organisational culture and the influence they have on behaviour. With this aim in mind, the current study examines how organisational culture exerts its influence over dysfunctional behaviour.

While many studies look into the influence of organisational culture as a single set of components affecting employee behaviour, this study takes a slightly different tangent. First, this study examines the influence of organisational culture as a higher-order factor to analyse its general effects. Later, organisational culture is disaggregated into four dimensions (see Cameron & Quinn, 2011; Quinn, 1988), allowing an in-depth investigation into how each culture dimension exerts its respective influence on behavioural intention.

2. LITERATURE REVIEW

2.1 Predicting dysfunctional behaviour

Dysfunctional behaviour, regardless of its magnitude, can potentially be harmful if it is not adequately addressed. Despite the seriousness of this matter, many employee dysfunctional behaviour incidents are not reported because they are either dealt with internally, or are swept aside due to the organisation's fear of negative market reactions, including those from customers.

Dysfunctional behaviour (and behaviour in general) is a function of multitudes of parameters. It is an expression of personal characteristics of the actor such as his or her traits, attitudes, interests, and more (Bergner, 2011). Behaviour has patterns and thus can be predicted. Based on theory of planned behaviour (TPB) (Ajzen, 1991, 2002a; Ajzen & Madden, 1986), *attitude*, *subjective norms*, and *perceived behavioural control* are good predictors of behavioural intention. Intention, in turn, is known to be a good precursor of actual behaviour (Ajzen, 1991, 2002a, 2002b, 2012; Ajzen & Madden, 1986; Armitage & Conner, 2001; Chang, 1998; d'Astous, François, & Montpetit, 2005). Measuring intention thus allows for a viable estimate of actual behaviour. Therefore, in the context of dysfunctional behaviour, intention not only is posited to have a significant relationship with (mis)behaviour, but also can be used to proxy actual behaviour.

TPB defines attitude as "…the degree to which a person has a favourable or unfavourable evaluation or appraisal of the behaviour in question" (Ajzen, 1991, p. 188). Thus, when an employee has a positive attitude towards dysfunctional behaviour, the stronger intention will be. In fact, many studies have found that attitude towards behavioural intention is the strongest among all predictors in TPB, regardless of whether the behaviour in the studies is security compliance (e.g., Jafarkarimi, Saadatdoost, Sim, & Hee, 2016; Leonard, Cronan, & Kreie, 2004; Sohrabi Safa, Von Solms, & Furnell, 2016) or dysfunctional.

Similarly, an increase in one's reliance on important others (which is governed by subjective norms (SN), a representation of a social factor influencing behaviour) can have a positive effect on intention. When important others are perceived as favouring an action, the employee's intention to engage in such behaviour becomes stronger. This is supported by Ifinedo (2012, 2014), who finds that SN has a positive effect on information security compliance behaviour, and a strong association with non-compliance actions which is demonstrated in the study by Barlow, Warkentin, Ormond, and Dennis (2013).

Another component of TPB is perceived behavioural control (PBC), which refers to a cognitive assessment of the ease or difficulty of performing the behaviour. PBC also brings about a vector toward intention similar to that of attitude and subjective norms. Ifinedo (2014) and Safa and Von Solms (2016) have found that behavioural control and self-efficacy positively affect employee IS compliance behaviour. Thus, in the context of dysfunctional behaviour, it can be derived that the stronger one's perception of control is, the stronger the intention is articulated.

2.2 Organisational culture influence on behaviour

Employee behaviour is not a sole output of one's volitional articulation of what one wants to do or ought to do. There are influences that shape one's actions, inducing a person to act in ways that are self-benefitting, or otherwise in the belief that a given act can be collectively favourable. In a context of an organisation, that influence is organisational culture, which exerts a systemic induction of one's behaviour. This is because organisational culture is a socially collective programming of minds (Hofstede, Neuijen, Ohayv, & Sanders, 1990), which encodes shared beliefs (Hu, Dinev, Hart, & Cooke, 2012; Schein, 1990) that characterise the sociology of an organisation (Davis & Pesch, 2013) upon which members' actions are governed.

Organisational culture further contributes to positive or negative impacts on organisational effectiveness or members of the organisation itself (Balthazard, Cooke, & Potter, 2006), and manifests itself in the form of physical or observable artefacts (Bloor & Dawson, 1994). These artefacts are visible through work practices, and the influence it exerts in management control system (MCS) design (see Dechow & Mouritsen, 2005), where the behavioural as well as decisional space of individuals in an organisation (Birnberg & Snodgrass, 1988) is limited in order to achieve the organisation's goals.

The influence of organisational culture on employee behaviour has been widely studied. For example, Tang, Li, and Zhang (2016), Van Niekerk and Von Solms (2010), and Boudreau, Serrano, and Larson (2014), posit that organisational culture is associated with employee behaviour. This is further supported by the work of Banerjee, Cronan, and Jones (1998) and Willison and Warkentin (2013), who discover a strong culture influence on employee decisional space when confronted with an ethical dilemma.

As organisational culture is a form of social influence, the myriads of this element affect one's reference on important others captured by subjective norms (SN) in theory of planned behaviour (TPB). The influence concedes in a way that when culture sanctions a given behaviour, the effect that subjective norms have on intention becomes stronger. Similarly, when the culture is seen as not in favour of certain actions, one's reference on important others is weakened, and hence so is the impact of SN on intention. The theorised role of organisational culture in the TPB model is illustrated in Figure 1. Here, organisational culture affects intent (together with attitude and perceived behavioural control) by intertwining with the subjective norm-intention relationship.

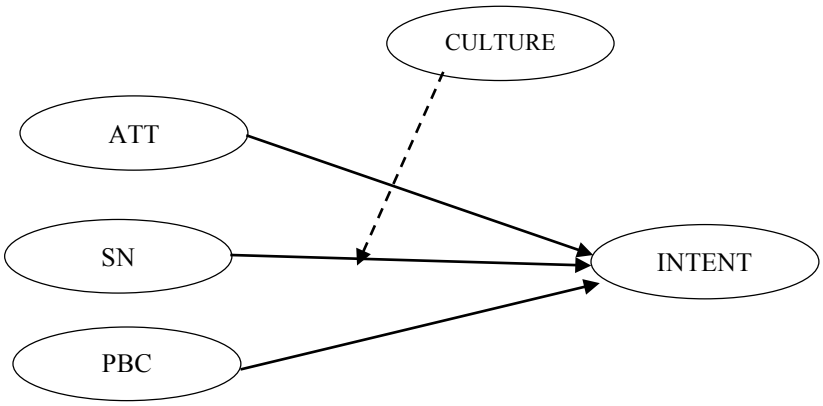

Fig. 1. Theoretical framework

Given organisational culture is important to employee behaviour, it is critical to know which aspects are more influential. As suggested by Bloor and Dawson (1994) and Schein (1990), the fact that organisational culture is a conjugation of shared beliefs which are realised in observable artefacts provides a strong connotation that it is a single factor at its higher order, and thus is decomposable at a lower order. Therefore, Quinn's (1988) culture

dimensions are coherent with this view. Quinn laid down a four-competing-value model inherited within the domain of organisational culture. These are *flexibility-control*, *innovation-rules*, *support-goal*, and *internal-external* focus orientations. Muijen et al. (1999) operationalise these four organisational culture dimensions into practical decompositions. The authors suggest flexibility-control (control) emphasises respect for authority, procedures, and hierarchical power. Innovation-rules (innovate) is characterised by efforts to search for new information, creativity, experimentation and a tendency to embrace changes. Support-goal (support) conceptualises the spirit of participation, people-based, team spirit and individual growth where employees are encouraged to express ideas about their work and feeling toward other members of the organisation. Internal-external focus (perform) embraces the concept of rationality, performance and accomplishments, accountability, and a reward system.

Many organisations resort to an extensive use of technological controls to attenuate the problem of insider misuse of IS. However, an indiscriminate approach of conventional formal control mechanisms is insufficient. Effective managerial control in a modern organisation needs to allow two competing values, control and flexibility (Cameron & Quinn, 2011; Quinn, 1988), which lay an emphasis on respect to authority and hierarchical power, to co-exist (Henri, 2006). This is a trade-off that some organisations are reluctant to make. Allowing flexibility by means of giving more freedom to employees to accomplish tasks creatively is normally done via relaxed security protocols. Less security measures often translate to less-than-effective internal control, from which perpetrators of IS crime can capitalise as evidenced in Baker et al.'s (2011) report. The strict down-top managerial approach, which also restricts propagation of innovative ideas, therefore leads this study to propose:

P1: The control dimension has a negative moderating effect on the subjective norm-intention relationship, in a way such that stronger control can weaken the impact of subjective norms on dysfunctional behaviour.

P2: The innovation dimension has a positive moderating effect on the subjective norm-intention relationship, in a way such that higher innovation can strengthen the impact of subjective norms on dysfunctional behaviour.

The third organisational culture dimension is support where it "…impacts employees on how they face their daily work intellectually and emotionally" (Shih, Lie, Klein, & Jiang, 2014, p. 671). This in turns, confers *esprit de corps* encouraging the employees to be dedicated and loyal to the organisation and strive to meet its goals (Shropshire, Warkentin, & Sharma, 2015). When approved behaviours are praised and support is provided, the employees identify (associate) themselves strongly with the group and the group norms and thus improve their dedication to the organisation. Similarly, when the support dimension is loosely convened and practiced, disassociation and discontent spark among employees, leading to dysfunctional behaviour (see Greene & D'Arcy, 2010). Therefore, this study proposes that:

P3: The support dimension has a negative moderating effect on the subjective norm-intention relationship, in a way such that stronger support can weaken the impact of subjective norms on dysfunctional behaviour.

The fourth dimension of organisational culture incorporated in this study is performance-reward scheme. This dimension is known to have an influence on employee behaviour in general as well as in information security related environments. Renaud and Goucher (2012), for example, observe this phenomenon in their study and conclude that security approved behaviour should be recognised and rewarded. Further, when the reward is clearly tied to performance, such a scheme provides an incentive for the employee to work toward achieving the goals set by the organisations. This method of management control helps to align employees' and the organisational objectives. When the performance-reward scheme is based on group performance, the goal congruence between members of the group with the organisation is achievable. And because of the group membership, where the influence of subjective norms on intention can be derived, such goal alignment can reduce individuals' dysfunctional behaviour. Therefore, this study argues that:

P4: The performance dimension has a negative moderating effect on the subjective norm-intention relationship, in a way such that stronger performance can weaken the impact of subjective norms on dysfunctional behaviour.

Clearly, the existing studies provide strong evidence for the notion that organisational culture indeed influences employee behaviour. However, this study differentiates itself from others by investigating four dimensions of organisational culture. The plethora of literature on organisational culture influence on dysfunctional behaviour suggests that each dimension affects behaviour differently. In this study, the four propositions suggested above were tested using anonymous survey instruments to provide further insights into employee dysfunctional behaviour in dealing with information system security practices.

3. METHODOLOGY

A total of 387 useable survey responses were sourced from employees of companies across Malaysia. The total data consisted of 23% from email (89 responses out of 380 email invitations) and 30% from mail (298 returned from 1000 mailed). The overall response rate was 28%, which is considered satisfactory in a survey-based study (see Baruch & Holtom, 2008).

Four vignettes, each with a different dysfunctional behaviour theme, were adapted from the work of D'Arcy (2007), corresponding to four taxonomies suggested by Stanton, Stam, Mastrangelo, and Jolton (2005). The use of vignette is designed to reduce issues of social desirability, common method bias and acquiescence bias (Crossler et al., 2013) by putting a comfortable distance between the respondents and the subject described in the vignette (Atzmüller & Steiner, 2010; Hughes & Huby, 2002; Schoenberg & Ravdal, 2000; Wason, Polonsky, & Hyman, 2002). Each questionnaire contains one vignette, with their potential confounding effects of individual vignette controlled for in the partial least square (PLS) analysis. Vignette 1 carried a theme of an unauthorised modification to an IS record, vignette 2 was designed on password sharing practices, and vignettes 3 and 4 were written on a basis of an unauthorised software installation and unauthorised access to IS, respectively.

The TPB variables were measured by the instruments adapted from studies by Ajzen (1991), Chatterjee (2008), Thompson, Higgins, and Howell (1991), and Venkatesh, Morris, Gordon, and Davis (2003). These variables are intention (INTENT: 5 items), subjective norms (SN: 3 items) attitude (ATT: 2 items), and perceived behavioural control (PBC: 5 items). Depending of their context, the TPB items were assigned either a 7-point scale from 'strongly disagree' to 'strongly agree', or from 'not at all' to 'all the time', or from 'very unlikely' to 'very likely'.

Four dimensions of organisational culture, i.e., *support, innovation, control* and *performance*, were measured using items adapted from Muijen et al. (1999). Subject to the question contextual imperatives, the respondents were asked to describe on a 7-point scale how many people in the organisation the event was applicable to ('nobody' to 'everyone'), or how often a certain event occurred ('never' to 'always').

The survey's administration was designed to address the issue of bias. Anonymity of the respondents was ensured explicitly in the invitation letter with no personally identifiable information being recorded. The use of vignettes added a further advantage by putting a psychological distance between the respondents and the persons committing dysfunctional behaviour.

Common method bias (CMB) was addressed statistically through the Harman's single factor test. All items used were loaded into principal component analysis (PCA) with the component extraction parameter set to 1. If CMB warranted a further control, a single-component factor should account for more than 50% of variance explained (Fullerton, Kennedy, & Widener, 2013; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003).

WarpPLS 5.0 was used as a primary analysis tool. This program estimates both measurement and structural models of the research. The quality of the measurement model was assessed through item reliability, convergent and discriminant validity, and overall reliability based on composite reliability estimates and Cronbach's alpha as well as variance inflation factor (VIF) to determine if multicollinearity is present in the model. The structural model was evaluated on its coefficient of determination, R^2, predictive relevant of the model through Stone-Geisser test, Q^2, structural path coefficients, β and their respective effect size, f^2.
Two models were analysed in this study. The first model looked at the moderating effects of organisational culture (CULTURE) the higher level of abstraction. Four CULTURE dimensions formed as indicators for this second-order level factor. In the second model, moderating effect of each CULTURE dimensions was examined to determine which dimension(s) exerted significant effects on the subjective norm-intention path.

4. RESULTS

The respondents were mostly in the 20 to 30 year old age group, with more than half being female. This demographic characteristic (i.e., age group) is expected as the sample was drawn from middle managers. Descriptive statistics for the respondents are summarised in Table 1.

Table 1. Sample descriptive statistics

	Vignette 1	**Vignette 2**	**Vignette 3**	**Vignette 4**	**Total**
Male	28	31	40	42	141
Female	44	74	58	70	246
Total	72	105	98	112	387
Age group:					
20 - 30	42	72	54	70	238
31 - 45	30	33	40	40	143
> 45			4	2	6
Total	72	105	98	112	387

Convergent and discriminant validities of the constructs are satisfactory as indicated by sufficient VIF of less than 5, composite reliability and Cronbach's alpha exceeding .70, and square-root of AVE are above the maximum correlations of the constructs. These measurement model parameters are summarised in Table 2 and Table 3.

Table 2. Constructs descriptive statistics, square-root of AVE and construct correlation

	Mean	SD	ATT	SN	INTENT	PBC	Support	Innovate	Control	Perform
ATT	3.580	1.890	(.975)							
SN	3.740	1.880	.772	(.954)						
INTENT	3.560	1.870	.770	.772	(.924)					
PBC	4.060	1.890	.637	.690	.710	(.872)				
Support	5.020	1.350	.174	.172	.109	.086	(.685)			
Innovate	5.290	1.490	.186	.148	.123	.166	.465	(.746)		
Control	5.740	1.120	.011	-.088	-.106	-.091	.502	.454	(.839)	
Perform	5.350	1.330	.108	.107	.081	.117	.515	.609	.599	(.778)

ATT = attitude, SN = subjective norm, INTENT = intention, PBC = perceived behaviour control.
Square-root of AVE is in parentheses on the diagonal.

Table 3. VIF, CR, and Cronbach's alpha of constructs

	VIF	CR	Cronbach's alpha
ATT	3.237	.974	.947
SN	3.467	.968	.968
INTENT	3.561	.967	.967
PBC	2.326	.941	.921
Support	1.817	.840	.771
Innovate	1.919	.883	.841
Control	2.256	.876	.787
Perform	2.351	.901	.868

VIF = Variance inflation factor, CR = Composite reliability.

The Harman's single component score test shows that total variance explained by a single factor was 22%. This suggests common method bias is not substantial enough to cause concern in this study, allowing a comfortable interpretation of the results.

The first model where moderating effect was analysed at its higher order level, indicates that organisational culture (CULTURE) moderates the causal path from subjective norm (SN) to intention (INTENT) ($\beta = .113$, $p < .05$, $f^2 = .034$). Attitude, subjective norm, and perceived behavioural control are all significant (ATT: $\beta = .472$, $p < .001$, $f^2 = .384$; SN: $\beta = .215$, $p < .001$, $f^2 = .167$; PBC: $\beta = .192$, $p < .001$, $f^2 = .137$).

In the second model, only control dimension has a positive moderating effect on SN-INTENT path ($\beta = -.107$, $p < .05$, $f^2 = .038$). Support, innovate, and perform do not exhibit statistical significance, although their beta coefficients indicate supports to the directions of moderating effects. The results of the decomposed organisational culture are summarised in Table 4.

Table 4. Results of structural paths of the second model

	INTENT		
	β	***f²***	***Propositions***
ATT	.488**	.397	
SN	.193**	.150	
PBC	.185**	.132	
Support*SN	-.015	.005	P3: Not supported
Control*SN	-.107*	.038	P1: Supported
Innovate*SN	.021	.005	P2: Not supported
Perform*SN	-.029	.009	P4: Not supported
$R^2 = .662$, *adj*. $R^2 = .655$, $Q^2 = .751$			

Table 4 also provides evidence of the model's predictive relevance (Q^2 = .751), with a combined effect of three predictors (and moderators) that explain 66% of the variation in intention to engage in dysfunctional behaviour (R^2 = .662, *adj*. R^2 = .655). According to Chin (1998), this level of variation in endogenous variable is one percentage point below the substantial level.

5. DISCUSSION AND CONCLUSION

Organisational culture is known to be a key influence on employees' behaviour in an organisation (Bloor & Dawson, 1994; Lacey, 2010). Which dimensions of organisational culture exert more influence than others remains a matter of a debate, in particular within the information system security domain. As organisations incorporate more and more computerised systems to cope with increasing transaction volume, the identification and prioritisation of the cultural dimension(s) shaping the way the employees interact with the systems becomes more critical.

The results show that attitude, subjective norms, and perceived behavioural control exhibit significant effects on the articulation of malicious intention. This study therefore, re-affirms what has been discovered in prior work where individual cognitive assessments help to shape employee behaviour. More precisely, the results also indicate that organisational culture moderates the effects of one's reference to important others (i.e., subjective norms) toward dysfunctional behaviour intention. The significant positive moderating effect of organisational culture on the subjective norm-intention structural path provides nominal support that once risky behaviour is routinised and widely practiced, such institutionalised atmospheric settings can strengthen the effect of employees' feeling that others will condone the intended dysfunctional behaviour. In practice, such organisation-wide tolerance can undermine the security net, leading to a compromised integrity of the information system assets.

Decomposing organisational culture into four identifiable facets further reveals how each dimension exerts its influence. Three out of four components of organisational culture (i.e., support, innovation, and performance) do not exhibit statistical significance, although their parameter vectors point to a direction consistent with existing literature and the propositions this study postulates. The support dimension, for example, points to a negative moderating effect, which means that as organisational support increases, the tendency of employee reliance upon important others leading towards dysfunctional behaviour is reduced. Similarly, the result for performance, which, among others, comprises a performance-reward initiative, also indicates that this dimension can help to weaken the subjective norm effect on dysfunctional behaviour when approved behaviour and good performance are rewarded.

Although this study does not find a statistical significant positive moderating effect of the innovation dimension, the fact that the control facet suggests a negative influence on the subjective norm-intention path indirectly conforms to a notion of the trade-off between freedom to innovate and hierarchical control instituted by management. The control dimension - which includes a strict adherence to procedures and authority, thus allowing little room for innovation to propagate - reduces the effects of the employee reliance upon others towards malicious behavioural intention. This result represents further evidence that formal control mechanisms sanctioned by management can help to reduce the exposure of information assets to risky behaviour.

Management control is important and has to become an integral part of organisational culture in order to effectively direct collective effort towards achieving the organisation's goals. Striking a balance between control and innovation in a view to reduce employee tendency towards dysfunctional behaviour is also critical. How much emphasis to be made in the control-flexibility continuum, and the other three dimensions of organisational culture remains a venue for future research to explore.

As a concluding remark, although the current study looks into less-than-serious dysfunctional behaviours, the impact of security transgression, no matter how small, can potentially be harmful if it goes unchecked. Future research, therefore, is encouraged to investigate more serious risky behaviour, such as intentional data manipulation, unauthorised access to and use of accounts with escalated administrative privileges, and data theft. This would help to enrich the existing knowledge on dysfunctional behaviour, leading to a strengthened information system security policy.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-t

Ajzen, I. (2002a). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. *Journal of Applied Social Psychology, 32*(4), 665-683. doi:10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I. (2002b). Residual Effects of Past on Later Behavior: Habituation and Reasoned Action Perspectives. *Personality and Social Psychology Review, 6*(2), 107-122. doi:10.1207/s15327957pspr0602_02

Ajzen, I. (2012). Martin Fishbein's Legacy: The Reasoned Action Approach. *The Annals of the American Academy of Political and Social Science, 640*(1), 11-27. doi:10.1177/0002716211423363

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology, 22*(5), 453-474. doi:10.1016/0022-1031(86)90045-4

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *The British Journal of Social Psychology, 40*, 471-499.

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences, 6*(3), 128-138. doi:10.1027/1614-2241/a000014

Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2011). *2011 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Balthazard, P. A., Cooke, R. A., & Potter, R. E. (2006). Dysfunctional culture, dysfunctional organization: Capturing the behavioral norms that form organizational culture and drive performance. *Journal of Managerial Psychology, 21*(8), 709 - 732. doi:http://dx.doi.org.ezproxy.ecu.edu.au/10.1108/02683940610713253

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly, 22*(1), 31-60.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39, Part B*(0), 145-159. doi:http://dx.doi.org/10.1016/j.cose.2013.05.006

Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations, 61*(8), 1139-1160. doi:10.1177/0018726708094863

Bennett, D. A. (2001). How can I deal with missing data in my study? *Australian and New Zealand Journal of Public Health, 25*(5), 464-469. doi:10.1111/j.1467-842X.2001.tb00294.x

Bergner, R. M. (2011). What is behavior? And so what? *New Ideas in Psychology, 29*(2), 147-155. doi:https://doi.org/10.1016/j.newideapsych.2010.08.001

Birnberg, J. G., & Snodgrass, C. (1988). Culture and control: A field study. *Accounting, Organizations and Society, 13*(5), 447-464. doi:10.1016/0361-3682(88)90016-5

Bloor, G., & Dawson, P. (1994). Understanding Professional Culture in Organizational Context. *Organization Studies, 15*(2), 275-295. doi:10.1177/017084069401500205

Boudreau, M.-C., Serrano, C., & Larson, K. (2014). IT-driven identity work: Creating a group identity in a digital environment. *Information and Organization, 24*(1), 1-24. doi:http://dx.doi.org/10.1016/j.infoandorg.2013.11.001

Brick, J., & Kalton, G. (1996). Handling missing data in survey research. *Statistical Methods in Medical Research, 5*(3), 215-238. doi:10.1177/096228029600500302

Cameron, K. S., & Quinn, R. E. (2011). *Diagnosing and Changing Organizational Culture : Based on the Competing Values Framework* Retrieved from http://ECU.eblib.com.au/patron/FullRecord.aspx?p=706769

Chang, M. K. (1998). Predicting unethical behavior: A comparison of the theory of reasoned action on the theory of planned behavior. *Journal of Business Ethics, 17*(16), 1825-1834.

Chatterjee, S. (2008). *Unethical behavior using information technology*. (Ph.D. 3370378), Washington State University, United States -- Washington. ABI/INFORM Complete; ProQuest Central; ProQuest Dissertations & Theses (PQDT) database.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), VII-XVI.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(0), 90-101. doi:http://dx.doi.org/10.1016/j.cose.2012.09.010

D'Arcy, J. P. (2007). *Misuse of information systems : The impact of security countermeasures*. New York, NY, USA: LFB Scholarly Publishing LLC.

D'Arcy, J. P., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658.

D'Arcy, J. P., & Hovav, A. (2009). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics, 89*, 59-71.

d'Astous, A., François, C., & Montpetit, D. (2005). Music Piracy on the Web - How Effective are Anti-Piracy Arguments? Evidence from the Theory of Planned Behaviour. *Journal of Consumer Policy, 28*(3), 289-310. doi:10.1007/s10603-005-8489-5

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers & Security, 68*, 1-15. doi:https://doi.org/10.1016/j.cose.2017.03.010

Davis, J. S., & Pesch, H. L. (2013). Fraud dynamics and controls in organizations. *Accounting, Organizations and Society, 38*(6–7), 469-483. doi:http://dx.doi.org/10.1016/j.aos.2012.07.005

Dechow, N., & Mouritsen, J. (2005). Enterprise resource planning systems, management control and the quest for integration. *Accounting, Organizations and Society, 30*(7–8), 691-733. doi:http://dx.doi.org/10.1016/j.aos.2004.11.004

Djajadikerta, H. G., Mat Roni, S., & Trireksani, T. (2015). Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research. *Information & Management, 52*(8), 1012-1024. doi:http://dx.doi.org/10.1016/j.im.2015.07.008

Fullerton, R. R., Kennedy, F. A., & Widener, S. K. (2013). Management accounting and control practices in a lean manufacturing environment. *Accounting, Organizations and Society, 38*(1), 50-71. doi:http://dx.doi.org/10.1016/j.aos.2012.10.001

Greene, G., & D'Arcy, J. P. (2010, 16-17 June 2010). *Assessing the impact of security culture and the employee-organisation relationship on IS security compliance.* Paper presented at the 5th Annual Symposium on Information Assurance 2010, New York.

Health effects of the Chernobyl accident and special health care programmes. (2006). Retrieved from Geneva: http://whqlibdoc.who.int/publications/2006/9241594179_eng.pdf

Henri, J.-F. (2006). Organizational culture and performance measurement systems. *Accounting, Organizations and Society, 31*(1), 77-103. doi:10.1016/j.aos.2004.10.003

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring Organizational Cultures: A Qualitative and Quantitative Study Across Twenty Cases. *Administrative Science Quarterly, 35*(2), 286-286.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences, 43*(4), 615-660. doi:10.1111/j.1540-5915.2012.00361.x

Hughes, R., & Huby, M. (2002). The application of vignettes in social and nursing research. *Journal of Advanced Nursing, 37*(4), 382-386. doi:10.1046/j.1365-2648.2002.02100.x

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi:http://dx.doi.org/10.1016/j.im.2013.10.001

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H., & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on Theory of Planned Behavior. *Computers in Human Behavior, 62*, 545-561. doi:http://dx.doi.org/10.1016/j.chb.2016.04.024

Karanja, E., Zaveri, J., & Ahmed, A. (2013). How do MIS researchers handle missing data in survey-based research: A content analysis approach. *International Journal of Information Management, 33*(5), 734-751. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2013.05.002

KPMG's fraud survey 2009, KPMG (2009).

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security, 18*(1), 4-13. doi:10.1108/09685221011035223

Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management, 42*(1), 143-158. doi:http://dx.doi.org/10.1016/j.im.2003.12.008

Liang, N., Biros, D. P., & Luse, A. (2016). An Empirical Validation of Malicious Insider Characteristics. *Journal of Management Information Systems, 33*(2), 361-392. doi:10.1080/07421222.2016.1205925

Mason, S., & Bohm, N. (2017). Banking and fraud. *Computer Law & Security Review, 33*(2), 237-241. doi:https://doi.org/10.1016/j.clsr.2016.11.018

Mat Roni, S. (2015). *An Analysis of Insider Dysfunctional Behaviours in an Accounting Information System Environment.* (Doctor of philosophy), Edith Cowan University, Joondalup.

Muijen, J. J. v., Koopman, P., Witte, K. D., Cock, G. D., Susanj, Z., Lemoine, C., . . . Turnipseed, D. (1999). Organizational Culture: The Focus Questionnaire. *European Journal of Work and Organizational Psychology, 8*(4), 551-568. doi:10.1080/135943299398168

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903. doi:10.1037/0021-9010.88.5.879

Quinn, R. E. (1988). *Beyond rational management: Mastering the paradoxes and competing demands of high performance* (1st ed.). San Francisco: Jossey-Bass.

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security, 20*(4), 296-311.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. doi:http://dx.doi.org/10.1016/j.chb.2015.12.037

Schein, E. H. (1990). Organizational culture. *American Psychologist, 45*(2), 109-119. doi:10.1037/0003-066x.45.2.109

Schoenberg, N. E., & Ravdal, H. (2000). Using vignettes in awareness and attitudinal research. *International Journal of Social Research Methodology, 3*(1), 63-74. doi:10.1080/136455700294932

Shih, S.-P., Lie, T., Klein, G., & Jiang, J. J. (2014). Information technology customer aggression: The importance of an organizational climate of support. *Information & Management, 51*(6), 670-678. doi:http://dx.doi.org/10.1016/j.im.2014.06.001

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*(0), 177-191. doi:http://dx.doi.org/10.1016/j.cose.2015.01.002

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security, 56*, 1-13. doi:10.1016/j.cose.2015.10.006

Spafford, E. H. (2014). Editorial. *Computers & Security, 43*, iv. doi:https://doi.org/10.1016/S0167-4048(14)00070-4

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133. doi:10.1016/j.cose.2004.07.001

Stoel, M. D., & Muhanna, W. A. (2011). IT internal control weaknesses and firm performance: An organizational liability lens. *International Journal of Accounting Information Systems, 12*(4), 280-304. doi:10.1016/j.accinf.2011.06.001

Tang, M., Li, M. g., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management, 17*(2), 179-186. doi:10.1007/s10799-015-0252-2

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly, 15*(1), 125-143.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486. doi:http://dx.doi.org/10.1016/j.cose.2009.10.005

Venkatesh, V., Morris, M. G., Gordon, B. D., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425-478.

Wason, K. D., Polonsky, M. J., & Hyman, M. R. (2002). Designing Vignette Studies in Marketing. *Australasian Marketing Journal (AMJ), 10*(3), 41-58. doi:10.1016/s1441-3582(02)70157-2

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly, 37*(1), 1-20.