Title: Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research

Author: Hadrian Geri Djajadikerta Saiyidi Mat Roni Terri Trireksani

PII: S0378-7206(15)00076-2
DOI: http://dx.doi.org/doi:10.1016/j.im.2015.07.008
Reference: INFMAN 2829

To appear in: *INFMAN*

Received date: 12-4-2014
Revised date: 5-6-2015
Accepted date: 15-7-2015

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

Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research

Highlights:

- We use a four-quadrant insider dysfunctional information system behavior taxonomy.
- We analyze intentions underlying behaviors among different dysfunctional behaviors.
- The intentions vary among dysfunctional information system behaviors.
- The causal links between behavioral intentions and their predictors vary.
- We address methodological concerns in the insider dysfunctional behaviors literature.

Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research

Hadrian Geri DJAJADIKERTA *

School of Business, Edith Cowan University, Australia

270 Joondalup Drive, Joondalup WA 6027, Australia

h.djajadikerta@ecu.edu.au

Saiyidi MAT RONI

School of Business, Edith Cowan University, Australia

270 Joondalup Drive, Joondalup WA 6027, Australia

m.matroni@ecu.edu.au

Terri TRIREKSANI

School of Management and Governance, Murdoch University, Australia

90 South Street. Murdoch WA 6150, Australia

t.trireksani@murdoch.edu.au

* Corresponding author
Address: Edith Cowan University, 270 Joondalup Drive, Joondalup WA 6027, Australia.
Tel.: +61 8 6304 5353
Email addresses: h.djajadikerta@ecu.edu.au (H.G. Djajadikerta)

Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research

ABSTRACT

Conflicting findings in the existing studies on insider dysfunctional information system (IS) behaviors have led some researchers to raise methodological concerns that samples in these studies are aggregated or disaggregated without sufficient attempt to differentiate their fundamental differences. Using a four-quadrant behavior taxonomy, this study investigates different types of dysfunctional information system behaviors to determine if, among them, there are any differences in behavioral intentions and in the causal links between these intentions and their predictor variables. The results show that both the intentions and the causal links between these intentions and their predictors vary among the four behavior categories.

Keywords:

Dysfunctional behavior taxonomy

Theory of planned behavior

Behavioral intention

Structural equation modelling

Partial least square

Vignettes

1. Introduction

Information system (IS) security risks posed by inappropriate actions of individual members of an organization have been a topic of interest in a vast amount of literature [1-3]. These individuals are insiders who sit behind the organizational firewall and are empowered with escalated user privileges [4]. They have a dual role in information security systems, both as allies and as a source of threats [5]. Studies have suggested that within the information security chain, insiders remain the weakest link in the effort to secure organizational IS assets [2, 3, 6, 7]. Some surveys and investigations have also shown that despite rapid advancement in protection technologies as well as IS security policies and procedures, IS security breaches remain significant and they are substantially linked to actions of insiders [8, 9].

The call for more studies on the behavioral aspects of IS security has long been voiced [4], and some significant studies exist in this area. The existing studies in the IS security area that look into the behavioral aspects of the insiders have provided insights into the effects of insiders' dysfunctional behaviors on organizational IS assets. These can be seen in valuable work on IS security compliance/non-compliance behaviors [10-20] including motivations to comply with IS security policies [21-24], IS misuse [2, 25-31], and studies on computer abuse [32-34]. These IS security studies, however, have largely focused on non-malicious and policy non-compliance behaviors [4, 7]. This leads to a further need for more studies into a broader range of actions that pose various levels of risk to organizational IS assets.

The following are some examples of the above studies. Myyry, Siponen, Pahnila, Vartiainen, and Vance [15] aimed to explain employees' IS non-compliance in terms of moral reasoning and values. Hu, Xu, Dinev, and Ling [16] described and tested a model of information security policy violation based on multiple criminological perspectives. Ifinedo [21] integrated social bonding, social influence, and cognitive processing perspectives to

understand employees' IS security policy compliance behaviors. Son [23] tried to explain why employees do or do not follow IS security rules using an intrinsic motivation model. Lowry, Posey, Bennett and Roberts [32] used fairness theory and reactance theory to explain why employees may blame organizations for and retaliate against improved IS policies.

In general, these studies can be aggregated as studies of IS security deviant behaviors within the context of volitional malicious and non-malicious behaviors [7, 11, 35]. This aggregated behavior typology, despite its usefulness, does not differentiate similar yet fundamentally disparate behaviors. For example, intentional IS record modifications within one's authorized workspace require less computer skills, while record changes requiring an escalated user privilege demand more computer knowledge to penetrate the internal firewall and to remove the digital footprint of such actions from log records. Consequently, control remedies such as instituting supervisory authorisation prior to record changes does not fully address the act of unauthorised record changes requiring high computer competency which demands protective control technologies to detect such attempts. The deviant behavior perspective therefore provides a foundation to understand negative insider behaviors at the aggregated level but fails to address typological differences at the subset level as behaviors are categorised only on a basis of intentions (i.e., malicious and non-malicious).

Consequently, investigating insiders' dysfunctional behaviors without applying an appropriate segregation of behavior categories could lead to sample contaminations, which render suggestions from the studies limited in practical use. Crossler, Johnston, Lowry, Hu, Warkentin, and Baskerville [6], and Posey, Roberts, Lowry, Bennett, and Courtney [36] have raised such methodological concerns citing that studies solely placing emphasis on improving security awareness among insiders cannot address the issues relating to insiders who engage in an act driven by malicious intentions. This is "because knowledge created from a focus on a single behavior or subset of behaviors does not necessarily generalize to the grand structure

of behaviors" [36, p.1190]. Their concerns are in line with Guo [37] and D'arcy and Herath's [38] suggestions that the studies in security-related behaviors in IS sometimes report inconsistent and contradictory results. The disparate findings were caused partly by a diverse conceptualisation of such behaviors in which "many of the concepts overlap with each other on some dimensions and yet are different on others" [37, p.242] and partly because factors explaining IS security compliance do not necessarily account for policy violations [37].

Taking the above discussion into consideration, this study tries to fill in the gap in the literature and aims to provide an indication of how dysfunctional information system behaviors at their aggregated and subset levels play a crucial role in information system security (mis)behavior. Overall, this paper searches for differences in behavioral intentions and in the cause-effect relationships between these intentions and their predictor variables among different types of dysfunctional information system behaviors. This paper accordingly addresses the above methodological issues in the current studies on insider dysfunctional behaviors in information systems [e.g., 4, 6, 36-38], allowing an examination of behavioral intentions and changes in the predictors of these intentions across different types of dysfunctional behaviors.

The next section of the paper reviews the conceptual discussion regarding dysfunctional information system behaviors, categories of insider behavior based on Stanton, Stam, Mastrangelo, and Jolton's [39] taxonomy, intention of dysfunctional behaviors, and the antecedents of intention. This conceptual discussion leads to the development of research propositions, which are subsequently described. It is followed by a presentation of research methodology and data employed in this study. This study uses vignettes in collecting the data through a survey to middle managers of medium sized enterprises (SMEs), and tests the model and analyzes the responses using partial least square structural equation modelling (PLS-SEM). Description and discussion of empirical results follow, where the study provides

important findings which show that both the intentions and the causal links between these intentions and their antecedents vary among different behavior categories. This paper concludes with a summary, limitations and future research opportunities that emerge from the study.

2. Conceptual discussion and proposition development

Some attempts to disaggregate seemingly similar behaviors have been demonstrated by Davis [40] who modelled two pathological internet uses/misuses with reference to their symptoms and effects. The work not only provides a general foundation to dysfunctional behavior classifications but also offers some understanding on how intricate connections of psychopathology (e.g., depression and social anxiety) and situational factors reinforce Internet users' cognitive approaches leading to Internet uses/misuses. Magklaras and Furnell [41] extended this concept by including computer skills as a part of their proposed user sophistication model, which advanced the identification and classification of dysfunctional behaviors.

Stanton et al. [39] proposed that the dysfunctional behaviors of interest should be mapped onto a two-dimensional plane, with the x-axis being the intensity of intentions (i.e., malicious to neutral to benevolent) and the y-axis being the level of computer skills required (i.e., low to high). Using this 2-vector plane, Stanton et al. [39], in their study, listed 94 behaviors which were later categorised into 6 types of behaviors, which include 4 risky types of insider behaviors (i.e., *intentional destruction, detrimental misuse, dangerous tinkering,* and *naïve mistake*) and 2 types of behaviors that are considered as acceptable practices (i.e., *aware assurance,* and *basic hygiene*). Their study is one of significant studies that has paved a way to aggregation and disaggregation of insider behaviors. These 6 types of behaviors are shown in Fig.1 with their descriptions summarized in Table 1.

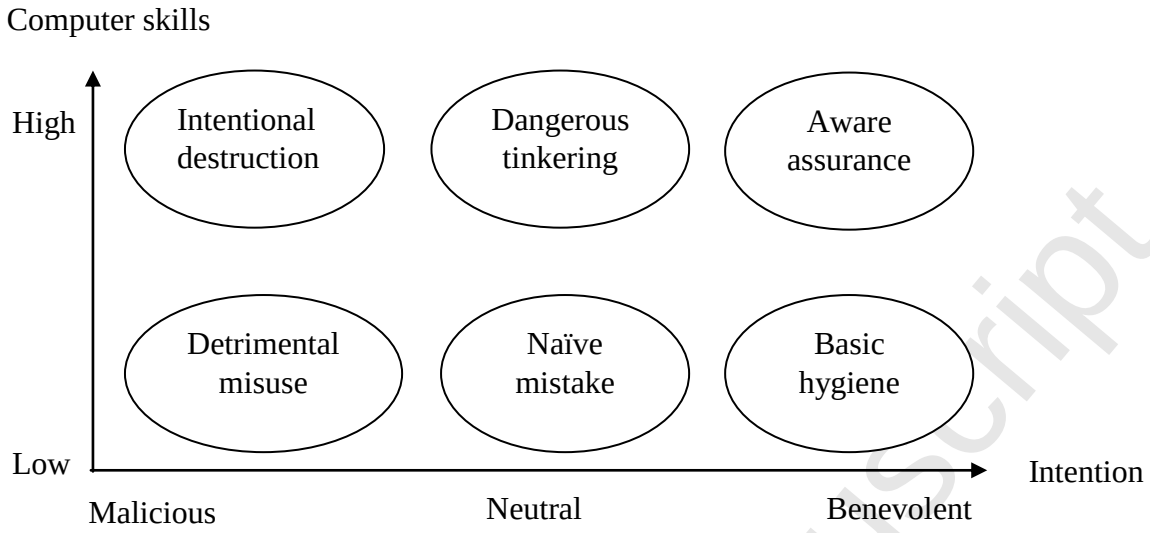

Fig. 1: Insider behavior categories *[39]*

Table 1: Description of behavior categories *[39]*

Behaviors	**Descriptions**
Intentional destruction	Requires high technical expertise together with a strong intention to harm organizational IS assets.
Detrimental misuse	Requires minimal technical expertise with a minimal intention to do harm through actions such as annoyance, harassment, and rule breaking.
Dangerous tinkering	Requires technical expertise but with no clear intention to do harm to organizational IS assets.
Naïve mistake	Requires minimal technical expertise with no clear intention to harm organizational IS assets.
Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting organizational IS assets.
Basic hygiene	Requires no technical expertise but includes a clear intention to preserve and protect organizational IS assets.

Recently, Guo [37] suggested eight indicators to identify the subsets of dysfunctional behaviors: (1) intentions (focuses on volitional/non-volitional action), (2) malicious/non-malicious, (3) level of computer skills and knowledge, (4) types of perpetrator, (5) job

relatedness, (6) direct or indirect damage to organizations, (7) requiring action or absence of actions by employees, and (8) actions are subject to policies.

To clearly layout the use of the insider dysfunctional behavior perspective in existing studies, relevant literature was analyzed to see how thematic behaviors were studied, how different types of behaviors were pooled together and/or separately examined, and where these behaviors reside within Stanton et al.'s [39] taxonomy (see Appendix A). The information in Appendix A highlights the general concerns raised by Crossler et al. [6], Posey et al. [36], Guo [37], Warkentin and Willison [4], and D'arcy and Herath [38] on the methodological issues in the existing studies on insider dysfunctional behaviors, particularly where samples are aggregated or disaggregated with limited or no attempt to differentiate their fundamental differences.

2.1. Using intention to capture dysfunctional behaviors

Intention has been recognized as a good predictor of actual behavior [42-44], driving a person to behave the way he/she does. The essence of the intention-behavior relationship is that the stronger the intention a person has, the more likely it is that the person will engage in the behavior [45, 46]. Intention is "assumed to capture the motivational factors that influence a behavior" [42, p.181]. It is an indication of "how hard people are willing to try, of how much effort they are planning to exert, in order to perform the behavior" [42, p.181]. Accordingly, intention is central to behavior, and it has been used widely as a proxy for actual behavior in situations when the behavior in question is difficult to be reliably or practically measured [e.g., in 44, 47, 48-50]. This is particularly the case when the behavior of interest is one that entails negative consequences such as disciplinary actions resulting from abusing organizational IS assets. Therefore, using intention to approximate actual behavior allows researchers to model their study to address actual (mis)behavior.

Utilising Stanton et al.'s [39] taxonomy (as shown in Fig. 1), this study uses a four-quadrant dysfunctional behavior taxonomy to serve as a basis for instrument development and analyses in this study. These four categories of dysfunctional behaviors are (1) *intentional destruction*, which requires a high level of computer skills and is accompanied with a malicious intention; (2) *detrimental misuse*, which includes a malicious intention but only requires a low level of computer skills; (3) *dangerous tinkering*, which requires a high level of computer skills but has a neutral intention; and (4) *naïve mistake*, which has a neutral intention and requires only a low level of computer skills. The other two categories of behaviors in Stanton et al.'s [39] taxonomy (i.e., aware assurance and basic hygiene) are not included in this study because these are considered benevolent or good practices.

2.2. Antecedents influencing dysfunctional behavioral intention

The theory of planned behavior (TPB) was used in this study in order to analyze dysfunctional behavioral intention at its grand structure and subset levels. TPB has been used to predict intention in many areas related to dysfunctional behaviors such as unethical use of IS [51], software piracy [30] and IS misuse [46]. Ajzen's description of TPB [42], seen in Fig. 2, showed intention as a construct in predicting actual behavior with attitude, subjective norms and perceived behavioral control as antecedents influencing intention.

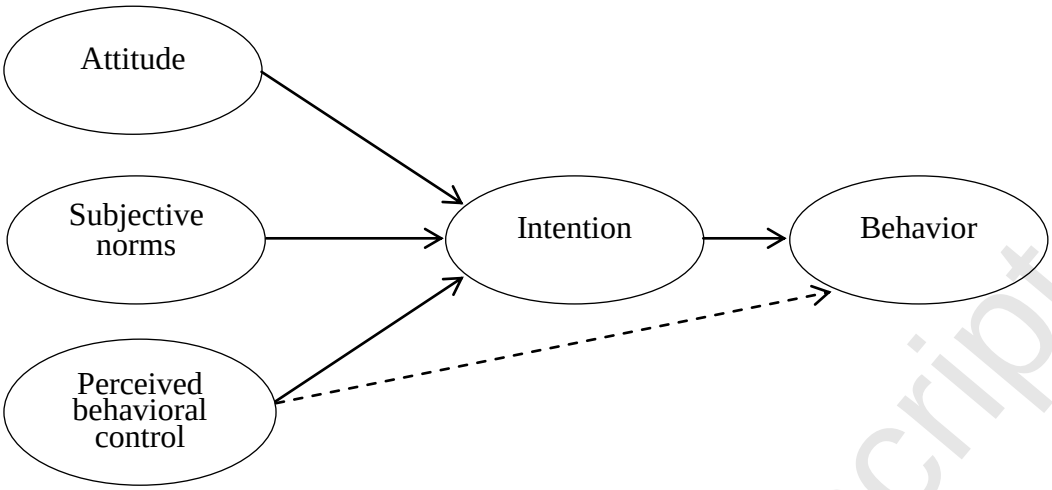

Fig. 2: Theory of planned behavior *[42]*

Attitude refers to an individual's preconceived cognition regarding a given behavior [42, 43, 52, 53]. The stronger the positive attitude towards a certain behavior, the higher the resulting intention to perform such behavior. This premise has been validated in many studies such as those of Hansen, Jensen and Solgaard [54], which predicted online purchase intention; Jimmieson, Peach and White [55], which ascertained employees' support for an organizational change; and Workman [46], which determined employees' use, disuse and misuse of an organization's expert and decision support systems.

Subjective norms refers to an individual's perception of important others' beliefs on whether she or he should engage in a given behavior [42, 43, 52, 53]. Well-aligned subjective norms tend to result in a stronger intention. It has been argued that a strong psychological contract creates a resilient bond between an individual and her or his reference group [55] resulting in a moral belief, which in turn becomes a robust predictor of intentions [30, 34, 56], even to the extent of contradicting one's attitude [57, 58].

Perceived behavioral control (PBC), on the other hand, is a subjective evaluation on how much an individual anticipates a level of control she or he has over behavior [52]. PBC is said to have attributes that reflect more of general external factors other than those

measured by self-efficacy [59]. However, PBC is not merely a single vector to intentions. The locus of control in PBC is a relative measure of how much control an individual has over resources to perform the behavior, which includes self-efficacy [see 60, 61, 62] and control over the outcomes of the behavior which are proxied as anticipated benefits [see 63].

The amount of control that an individual has over the relevant resources is translated into a stronger intention to perform a given behavior. This premise has been reflected in components of many other theories such as effort-expectancy in unified theory of acceptance and use of technology (UTAUT) [45], perceived-ease-of-use in technology acceptance model (TAM) by Davis [64], and complexity in innovation diffusion theory (IDT) [65]. Similarly, the higher level of perceived control an individual has over anticipated favorable outcomes of a certain behavior for her or himself, the more likely that her or his intention to perform such behavior converges [66] because the outcomes are viewed as a reward for the risk taken in performing the behavior [58].

Despite its efficacy, TPB has appeared to be non-resilient due to conflicting findings in various studies, especially in predicting insider dysfunctional behaviors with negative consequences. For example, in a study conducted over online purchase intention, Hansen et al. [54] found that, although attitude and subjective norms exhibited strong effects on intention, PBC had a small or non-significant effect on intention. This indicates that variations in intentions may be further explained by other factors beyond what the three TPB predictors (i.e., attitude, subjective norms and perceived behavioral control) have accounted for. Tsohou, Karyda, Kokolakis, and Kiountouzis [5], Wang, Gupta and Rao [67], and Kraemer, Carayon and Clem [68] for example, suggested organizational and technological factors to be examined.

As one type of behavior could form an alternative course of action of, or reciprocal to, the other type of behavior [see 69], the relationships between attitude, subjective norms,

perceived behavioral control and subsequent intention to perform a given behavior could also change. This perspective gives a strong indication that each type of (mis)behavior should be studied separately rather than in a single pool of categories. In order to systematically study different, yet related, types of behavior, a proper approach or taxonomy has to be used. Stanton et al.'s [39] taxonomy, which categories four-quadrant dysfunctional behaviors, is suitable to be used for this purpose. Within this taxonomy, a variation in the effects of TPB predictor constructs (attitude, subjective norms, and perceived behavioral control) could be posited as a result of different intensities of intentions and different levels of computer skills within what are otherwise a similar set of behaviors. By implementing this dysfunctional behavior taxonomy, which is based on a 2-vector dimension, this study expects to find empirical support to strengthen suggestions from previous scholars [e.g., 4, 6, 36, 37] that different types of dysfunctional behaviors have to be studied separately. Therefore, this study develops propositions as follows.

Proposition 1: *The intentions underlying behaviors vary among different types of dysfunctional information system behaviors.*

Proposition 2: *The causal links between the TPB factors (i.e., attitude, subjective norms and perceived behavioral control) and the intentions underlying behaviors vary among different types of dysfunctional information system behaviors.*

Overall, this study tries to investigate different types of dysfunctional information system behaviors to determine if there are any differences among them in behavioral intentions and in the cause-effect relationships between the TPB predictor variables and these intentions. This study accordingly addresses the concerns on the methodological issue where sample contaminations may limit the usefulness of prior studies on information security [4, 6, 36, 37].

3. Methodology

3.1. Vignettes and scale development

Studies that involve values and norms have always posed difficult methodological questions to achieve a certain level of internal validity (Finch, 1987). The widely used solution to this methodological challenge is to present respondents with vignettes, which are short description s of hypothetical scenarios that comprise the essential information for respondents to base their judgments upon. In this study, four vignettes, each with a different theme, were adapted from the work of D'Arcy [70] to conform to the four dysfunctional behavioral categories in the taxonomy suggested by Stanton et al. [39] that were used in this study. The use of vignettes is crucial to this study to alleviate social desirability, common method bias and acquiescence bias [6] by putting a comfortable distance between the respondent and the subject described in the vignette [71-74].

To develop vignettes uniquely responsive to specific topical applications and to improve their internal validity, a careful design is needed to create context-sensitive, realistic and familiar scenarios [73]. Although a vignette is hypothetical and commonly involves a 'fictitious third person', the closer the vignette is able to relevantly and accurately depict an individual's situation, the more sensitive and effective the instrument will perform [75]. D'Arcy [70] carefully chose and tested four IS misuse vignettes in their study since they are considered nonintrusive, and hence provided a comfortable way for the respondents to answer. This paper adapted and modified these vignettes, and included the following four vignettes in the survey: (1) unauthorized modification of computerized data – portrayed intentional destruction behavior; (2) unauthorized access to computerized data – portrayed detrimental misuse behavior; (3) unauthorized unlicensed software installation – portrayed

dangerous tinkering behavior; and (4) unauthorized password sharing – portrayed naïve mistake behavior.

These vignettes depicted hypothetical situations that required relatively low to moderate levels of malicious intention and computer skills. Therefore, the relative differences among the four vignettes in terms of either computer skills and/or malicious intention are rather moderate. However, they provided more realistic and familiar scenarios that could relevantly and accurately portray the respondents' daily situation, and hence could result in improved internal validity [50, 76].

The TPB variables (i.e., intention, attitude, subjective norms and perceived behavioral control) were measured by the instruments adapted from previous studies of Azjen [42], Chatterjee [51], Thompson, Higgins and Howell [66], and Venkatesh, Morris, Gordon and Davis [45]. These variables are intention (INTENT), which was measured using 5 items, subjective norms (SN) which was measured using 3 items; attitude (ATT), which was measured using 2 items; and perceived behavioral control (PBC), which was measured using 5 items.

It has been posited that organizational culture is associated with employee behavior, binding the organization's members with complex beliefs, expectations, ideas and values [77]. In order to control for the effect of organizational culture, four dimensions of organizational culture, i.e., *support*, *innovation*, *practice* and *performance*, were measured using items adapted from Muijen, Koopman, Witte, Cock, Susanj, Lemoine, Bourantas, Papalexandris, Branyicski, Spaltro, Jesuino, Neves, Pitariu, Konrad, Peiró, González-Romá and Turnipseed [78]. These dimensions formed a higher-order factor, which was used as a control variable (CULTURE).

The items measuring CULTURE and TPB components are summarized in Appendix B. All of these items were measured using a 7-point scale. 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', For the CULTURE items, the respondents were asked to describe on a 7-point scale how many people in the organization the event was applicable to ('nobody' to 'everyone'), or how often a certain event occurred ('never' to 'always').

The instrument containing all four vignettes and the TPB items was pre-tested on eight middle managers to examine the overall structure of the instrument. Considering feedback received from the pre-test, two additional items were added to the initial three items adapted from Chatterjee [51] and Venkatesh et al. [45] on the intention construct. These two items were developed to better capture the overall notion of dysfunctional behavioral intention. The revised questionnaire and the vignettes were subsequently pre-tested on 38 middle managers to assess the reliability of the items in the revised instrument. Four sets of questionnaires were prepared, each attached with one vignette from one of the four types of dysfunctional behaviors in the taxonomy. Ten questionnaires for each set were sent to the respondents, and two of the forty respondents did not return the questionnaires. The results of this second pre-test showed a set of satisfactory loadings on the components and a sufficient reliability of the instrument for the actual study with Cronbach's alpha ranging from 0.77 to 0.98.

The variables used in this study and their items are described in Appendix B. The vignettes, themes and relevant dysfunctional behavior types are summarized in Appendix C.

3.2. Sample and data collection

The sample used in this study was middle managers of medium sized enterprises (SMEs) in Malaysia. The list of companies was obtained from SME Corp of Malaysia, which is a central agency for SMEs, commissioned by the Malaysian government to formulate

policies and coordinate programs among other agencies relevant to the SMEs. Medium size companies were chosen for this study since companies this size have normally developed a unique organizational culture, but not one so large that the culture becomes disparate from one department to another [79]. This study also focused on companies in three sectors (i.e., service, retailing and manufacturing) which were chosen for their volume of transactions and extensive use of IS. Finally, the middle manager group was chosen since staff within this group were commonly provided with an IS user privilege or system access which presented an opportunity to (mis)use the system.

412 responses were collected from 1380 survey questionnaires mailed and emailed. Each survey questionnaire sent to the respondent was attached with only one of the four vignettes, which was randomly assigned. Responses with a missing data percentage of more than 20% were excluded [1, 80, 81]. 91 responses were received from the email-based survey, and 2 responses were excluded because of missing data. 321 responses were received through the mailed survey, and 23 responses were excluded because of missing data. The total 387 useable responses were represented by 23% from email (89 responses out of 380 email invitations) and 30% from mail (298 returned from 1000 mailed invitations).

The overall response rate was 28%, which was considered satisfactory in a survey-based study. Baruch and Holtom [82] conducted an extensive review comprising 1607 journal articles and found that an average response rate for a survey within organizational research stood at 36% with a standard deviation of 18.8. Other studies suggested that response rates for mail-based email-based surveys could be as low as 21% and 10%, respectively [see 1, 83]. The data collection was conducted for a 5-month period beginning in February 2013. Descriptive statistics of the responses are shown in Tables 2 and 3 below.

Table 2: 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
	72	105	98	112	387

Table 3: Item descriptive statistics

	Mean	Std. Dev.	Median
att1	3.445	1.924	3
att2	3.585	1.890	4
sn1	3.788	1.845	4
sn2	3.737	1.883	4
sn3	4.065	1.748	4
pbc1b	4.057	1.887	4
pbc2b	4.109	1.907	4
pbc1a	4.376	1.822	5
pbc2a	4.283	1.804	5
pbc3a	4.433	1.721	5
int1	3.506	1.878	4
int2	3.556	1.868	4
int3	3.44	1.959	4
int4	3.518	1.991	4
int5	3.497	2.019	3

3.3. Data analysis

Data was initially analyzed using *t*-tests to see if there were any significant differences in the mean values of the constructs between the two modes of survey distribution (i.e., mail-based and email-based). The results show that there were no significant differences between mail and email responses for all items (see Appendix D).

Exploratory factor analysis (EFA) was subsequently performed to determine factorial validity of the items. The EFA was conducted using principal component analysis extraction with oblique rotation. The result from the EFA was used as a basis for the development of the latent constructs in subsequent analyses.

Partial least square structural equation modelling (PLS-SEM) was later used to test the full research model, which included behavior types (VIGNETTE) and organizational culture (CULTURE) as control variables. PLS-SEM is used in this study due to the nature of the approach that seeks to maximise the explained variance in the dependent latent construct (in this case, intentions) for predictive and theory development purposes [84, 85]. Despite TPB being widely acknowledged for its efficacy, the main objective of this study is to look into different types of dysfunctional information system behaviors, and search, among them, for differences in intentions underlying behaviors and in the cause-effect relationships between the TPB predictor variables and these intentions.

In a pursuance of this objective, PLS-SEM is preferred in this study as the method provides advantages over first generation statistical techniques (e.g., correlation and regression) and covariance-based SEM (CB-SEM) for theory building [86]. PLS-SEM incorporates several statistical techniques that are not part of CB-SEM, resulting in more reliable parameter estimates in exploratory analysis required for theory building [87-89] without inflating the *t*-statistic [86]. The advantage of PLS-SEM in theory building is further enhanced by the availability of *modes* in PLS that define specific algorithms to be used to output parameter estimates appropriate for specific research situations [90].

PLS-SEM also allows "constructs with fewer items (e.g., one or two) to be used" since "the constructs' measurement properties are less restrictive with PLS-SEM" comparatively to that of CB-SEM [84, p.140]. Additionally, PLS-SEM is arguably found to be useful in dealing with research model that incorporates higher-order constructs [86]. The

control variable used in this study, i.e., CULTURE, was a second-order construct, providing further reason for the use of PLS-SEM in this study.

Three commonly available modes in PLS-SEM analysis are (1) *Mode A* which is equivalent to correlation weights to optimise out-of-sample prediction [90], (2)*Mode B* which is regression weights equivalence using multiple ordinary least square (OLS) regressions that optimise R^2 [91], and (3) *PLS regression* mode which does not allow estimates of inner model to influence outer model parameters [92] resulting in a more stable and better interpretable alternative to OLS particularly in a view of multicollinearity [93]. In this study, the PLS regression mode was used to reduce potential collinearity effect.

A two-step approach on PLS-SEM was used in the analysis following suggestions by Anderson and Gerbing [94], and Hair Jr, Sarstedt, Hopkins and Kuppelwieser [89]. This step requires assessments on the measurement and the structural models. The assessment criteria for both measurement and structural models are summarized in Tables 4 and 5. WarpPLS version 4.0 was used in this study. Among many features offered, this software estimates *p*-values for path coefficients automatically and also provides variance inflation factor (VIF) for latent constructs allowing an easy assessment for multicollinearity issue in the research model.

Table 4: Measurement model assessment criteria

Assessments	Criteria	Notes	References
Item reliability	Individual item standardised loading on parent factor.	Min. of 0.50	Hair, Black, Babin and Anderson [95]
Convergent validity	Individual item standardised loading on parent factor, and	Min. of 0.50	Hair et al. [95]
	Loadings with sig. *p*-value	$p < 0.05$	Gefen and Straub [96]
	Composite reliability	> 0.70	Fornell and Larcker [97] Nunnally and Bernstein [98] Hair et al. [95]
	Average variance extracted (AVE)	> 0.50	Hair et al. [95] Urbach and Ahlemann [99]
Discriminant validity	Square-root of AVE	More than the correlations of the latent variables.	Hair et al. [95]
Reliability	Cronbach's alpha	> 0.70	Nunnally and Bernstein [98] Urbach and Ahlemann [99] Hair et al. [95]
	Variance inflation factor (VIF)	< 10	Hair et al. [95]
		< 5	Kock and Lynn [100]
Nature of construct	Formative / reflective:		Chin [87] Coltman, Devinney, Midgley and Veniak [101]

Table 5: Structural model criteria

Criteria	Notes	References
Coefficient of determination, R^2	0.67 substantial 0.33 average 0.19 weak	Chin [87]
Predictive relevance, Q^2	> 0 Stone-Geisser test	Geisser [102] Stone [103]
Effect size, f^2	0.02 small 0.15 medium 0.35 large	Cohen [104]
Path coefficient	Assessed on: Magnitude Sign p-value	Hair et al. [95]

4. Results and discussions

4.1. Exploratory factor analysis (EFA)

A principal component analysis (PCA) with oblique rotation was run as an initial test on items correlations. 9 components were extracted based on eigenvalue more than 1. These included 4 components of organizational culture (CULTURE) and 5 components of the TPB. For CULTURE, 21 items loaded into 4 distinct components, i.e., support comprised of 6 items, innovation of 6 items, practices of 3 items, and performance of 6 items. For TPB, 13 items loaded into 5 distinct components, i.e., intention (INTENT) comprised of 3 items, subjective norms (SN) of 3 items, attitude (ATT) of 2 items, and the remaining 5 items measuring perceived behavioral control (PBC) loaded into two components which were labelled as perceived behavioral control over outcomes of behavior (PBC-Out) with 2 items, and perceived behavioral control over resources to engage in behavior (PBC-Res) with 3 items. The list of items for PBC-Out and PBC-Res is provided in Appendix 3.The PCA results on PBC suggest that PBC is not a single construct. It is rather a function of two first-

order constructs – perceived control over the resources and perceived control over outcomes of the behavior. This corroborates indications from previous studies [45, 60-63, 65, 66].

4.2. Measurement model assessment

The measurement model was assessed with reference to criteria in Table 4. Individual item reliability was confirmed with item standardised loading on parent factor achieving a minimum value of 0.50 (see Appendix E). As demonstrated in Appendix E convergent validity was also achieved with significant items loading (p-value < 0.001). Further, convergent validity was also confirmed with composite reliability for all latent constructs of more than 0.70 and average variance extracted (AVE) of more than 0.50 as shown in Table 6. The instrument's reliability was demonstrated with sufficient Cronbach's alpha of more than 0.70 and variance inflation factor (VIF) of less than 5.

Table 6: Latent variable coefficients

	ATT	SN	PBC-Out	PBC-Res	INTENT	CULTURE
R^2					0.732	
Adjusted R^2					0.728	
Composite reliability	0.974	0.968	0.980	0.905	0.967	0.878
Cronbach's alpha	0.947	0.951	0.958	0.841	0.957	0.815
AVE	0.950	0.911	0.960	0.761	0.853	0.644
Full collinearity VIF	3.122	3.299	3.601	3.005	3.512	1.040
Q^2					0.742	

AVE = Average variance extracted, VIF = Variance inflation factor

The measurement model also demonstrated sufficient discriminant validity with square-root of AVE of latent constructs exceeding their respective inter-construct correlation. This is shown in Table 7. It is also noted in Table 7 that PBC-Out and PBC-Res exhibited relatively high correlation of .81 despite higher square-root of AVE values. The constructs

was maintained as two distinct constructs based on VIF assessment of less than 5 and AVE of more than 0.50 [see 105].

Table 7: Latent variable means, standard deviations, square-root of AVEs and correlations

	Mean	SD	ATT	SN	PBC-Out	PBC-Res	INTENT	CULTURE
ATT	3.515	1.907	**0.975**					
SN	3.863	1.830	0.772	**0.954**				
PBC-Out	4.083	1.896	0.642	0.681	**0.980**			
PBC-Res	4.364	1.782	0.574	0.636	0.806	**0.872**		
INTENT	3.501	1.901	0.770	0.772	0.711	0.643	**0.924**	
CULTURE	5.193	1.355	0.148	0.105	0.094	0.071	0.064	**0.802**

Square-root of AVEs are in bold on the diagonal.

4.3. Structural model assessment

A full structural model, shown in Fig. 3, was run for a full dataset [see 11, 20, 28]. The structural model was assessed based on coefficient of determination (R^2), predictive relevance (Q^2), effect size (f^2) and magnitude and sign (β) and p-value of path coefficient as summarized in Table 7.

The full structural model showed that four predictors accounted for 73% of variation in INTENT (R^2= 0.73), after controlling for organizational culture (CULTURE) and effects of behavior types (VIGNETTE). According to Chin [87], R^2 of this magnitude is considered substantial. A Stone-Geisser test also showed that the model has sufficient predictive relevance (Q^2 = 0.74). These R^2 and Q^2 figures indicate a highly predictive model.

The result further showed that structural paths leading from the predictors to the criterion (INTENT) were all significant with ATT having the largest impact on INTENT in both magnitude and effect size (β = 0.45, p < 0.001, f^2= 0.37). SN, on the other hand, had a medium effect on INTENT (β = 0.24, p < 0.001, f^2= 0.19), while two components of perceived behavior control, despite their statistical significances, both demonstrated relatively

weak effects (PBC-OutC: β = 0.10, p = 0.02, f^2= 0.07; PBC-Res: β = 0.13, p = 0.002, f^2= 0.08).

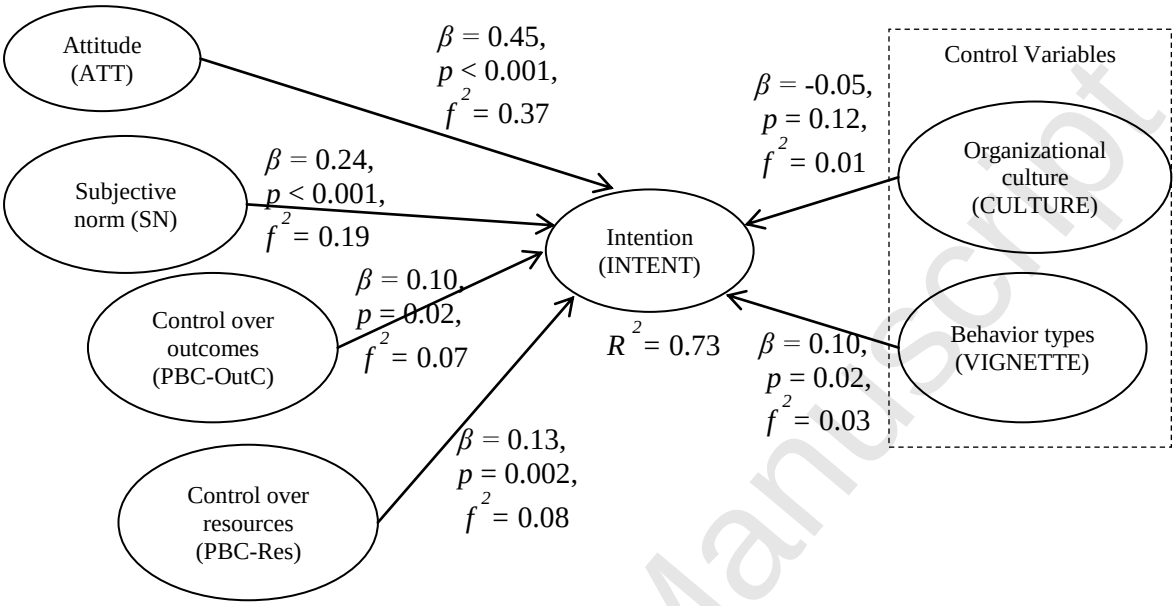

Fig. 3. Full structural model

4.4. Intentions among different types of dysfunctional information system behaviors

A one-way between groups analysis of variance (ANOVA) was used to investigate differences in behavioral intentions among the four dysfunctional information system behavior types. As the sample size for each vignette was relatively unequal, post hoc ANOVA analyses were set with Gabriel's procedure [106] to account for the differences. Levene's test also indicated homogeneity of variance could not be assumed in this analysis (F (3, 383) = 4.966, p = 0.002). Therefore, contrast test was read from unequal variance value set to preserve conservative estimate.

The result of the ANOVA was statistically significant, indicating that there are differences in behavioral intentions among the four types of dysfunctional information system behaviors (F (3, 383) = 10.51, p < 0.001). Post hoc tests further revealed that dangerous tinkering (M = 4.29, SD = 1.70) had a significantly higher impact on intention

compared to the impacts of naïve mistake (M = 3.08, SD = 1.70), detrimental misuse (M = 2.99, SD = 1.73) and intentional destruction (M = 3.55, SD = 1.97) on intention. However, no significant mean differences were found between naïve mistake, detrimental misuse and intentional destruction. The mean differences and their respective effect sizes are summarized in Table 8. These results support Proposition 1 that the intentions underlying behaviors vary among different types of dysfunctional information system behaviors.

Table 8: Mean differences, significance levels and effect sizes

(I) Vignettes	(J) Vignettes	Mean differences (I-J)	Std. error	Sig.	Contrast levels	Effect size, *d*
Dangerous tinkering	Naive mistake	1.21	0.28	0.000	1	0.44
	Intentional destruction	0.74	0.25	0.018	2	0.30
	Detrimental misuse	1.30	0.25	0.000	3	0.53
Detrimental misuse	Naive mistake	-0.09	0.27	1.000	4	0.03
	Intentional destruction	-0.56	0.24	0.123	6	0.24
Naive mistake	Intentional destruction	-0.47	0.27	0.395	5	0.18

Dependent Variable: INTENT

In order to test for differences in the cause-effect relationships between the TPB predictor variables and behavioral intentions among the four types of dysfunctional information system behaviors, a separate PLS-SEM was run for each vignette with CULTURE as a control variable. The results of the PLS-SEM analysis, together with R^2 and adjusted R^2 values for each behavior type are summarized in Table 9.

Table 9: Path coefficients, R^2 and adjusted R^2

	R^2	adjusted R^2	ATT	SN	PBC-Out	PBC-Res
Vignette 1: Naïve mistake	0.734	0.714	0.170*	0.287*	0.365**	0.005
Vignette 2: Detrimental misuse	0.780	0.769	0.544**	0.225*	0.105	0.071
Vignette 3: Dangerous tinkering	0.831	0.822	0.616**	0.035	0.011	0.323**
Vignette 4: Intentional destruction	0.853	0.846	0.626**	0.302**	0.031	0.050

Dependent variable: INTENT. * Significant at $p < 0.05$, **Significant at $p < 0.001$

INTENT = Intention, ATT = Attitude, SN = Subjective norms, PBC-OutC = Perceived behavioral control over outcomes, PBC-Res = Perceived behavioral control over resources

It can be seen from the results that the significant effects of each predictor variable on intention vary for each vignette. Across all four vignettes, only the causal link between attitude and intention remained significant. Subjective norms did not have a significant effect on intention in the dangerous tinkering type of behavior, but it significantly affected intention in the other three types of behaviors. The cause-effect relationships between perceived behavioral control over outcomes and perceived behavioral control over resources on intention changed in varying degrees for each type of dysfunctional behavior. Perceived behavioral control over resources only had a significant effect on intention in the dangerous tinkering type of behavior, while perceived behavioral control over outcomes was observed to only affect intention in the naïve mistake type of behavior.

These PLS results show that the cause-effect relationships between the predictor variables and behavioral intentions among the four types of dysfunctional information system behaviors are different. The changes in magnitude and significance of the paths leading from predictor variables to intention for each behavior category therefore support Proposition 2,

which states that the causal links between the TPB factors (i.e., attitude, subjective norms and perceived behavioral control) and the intentions underlying behaviors vary among different types of dysfunctional information system behaviors.

5. Conclusion

The results of this study suggest that both the intentions underlying behaviors and the causal links between the TPB factors and these intentions vary among the four types of dysfunctional information system behaviors. These provide empirical support for the methodological concerns and fill the gap in the literature on insider dysfunctional behaviors, where samples are aggregated or disaggregated without sufficient attempt to differentiate their fundamental differences [see 4, 6, 36, 37]. The results also show that the level of intention in the dangerous tinkering type of behavior is significantly higher compared to the levels of intention in the other three types of dysfunctional behaviors (i.e., intentional destruction, detrimental misuse and naïve mistake). The dangerous tinkering vignette that was used in this study illustrates an unauthorised installation of application into an organization's computer, which requires high computer skill and assumes high consciousness in order to perform the unwarranted action. This could indicate that perpetrators who have a high level of computer skills may tend to engage in this type of dysfunctional behavior since they feel that their intentions are not malicious. From the organizational viewpoint, this kind of behavior certainly can pose substantial threats to the integrity of an entity's information system (IS).

Looking at the three TPB antecedents (i.e., attitudes, subjective norms, and perceived behavioral control) that were analyzed in this study, it is found that regardless of the level of computer skills (i.e., low or high) and intentions (i.e., malicious or neutral) the attitude construct remains significant across all of the four types of dysfunctional behavior used in

this study. Ajzen and Fishbein [42] and Armitage and Conner [59] concur that attitude is a result of attitudinal belief which can reside within an individual and be moulded by many factors. This finding should bring the focus of organizations towards effectively shaping their employees' attitudes and preventing inappropriate behaviors against IS security policy. As such, security awareness programs [107-109] form one of the many approaches available for organizations to influence their employees' attitudinal belief, which in essence influences attitude.

The subjective norms construct is significant within three dysfunctional behaviors in the four-quadrant dysfunctional behavior categories: intentional destruction (a malicious intention requiring high computer skills), detrimental misuse (a malicious intention requiring low computer skills) and naïve mistake (no clear intention requiring low computer skills). The dangerous tinkering type of behavior does not exhibit any significant reliance on subjective norms. These findings show that subjective norms become an important factor when a perpetrator's intention is clearly malicious (i.e., intentional destruction and detrimental misuse) or intentionally ignoring. From an organizational point of view, when an employee is confronted with a dilemma either to engage in dysfunctional behavior or to refuse it altogether, a work environment, which forms a basis of reference to important others, plays an important role [see 110, 111, 112]. If the employee feels important others would take similar (unwarranted) action, it is very likely that he or she will engage in IS security malpractices.

When the intention is unclear, it is the individual's perceived behavioral control (PBC) that matters. Many studies [e.g., 21, 44, 113] have treated PBC as a single construct, and accordingly much valuable information has been lost in the analysis. This study finds that PBC is a function of control over resources required to perform a given behavior and control over the outcomes resulting from the performance of a given behavior. Analysing the path

leading from these two components of PBC to behavioral intentions could create more output which allows an organization to better address insider dysfunctional behavior when working with IS.

On the contribution to the understanding of TPB, where it apparently fails to predict behavior, carefully examining the situational conditions in which the behavior of interest is located may be able to augment the research in question. When two or more behavior types are studied together, each of them has to be screened for its inter-changeability and reciprocity with the others. The results of this study support the concerns of Crossler et al. [6], Posey et al. [36], Warkentin and Willison [4], and D'arcy and Herath [38] which suggested contaminations of the samples in the existing studies of insiders' dysfunctional behaviors in the information security discipline. Therefore, future studies in this field are encouraged to take into consideration the fine lines that separate seemingly similar, yet fundamentally different, types of behaviors in order to have suggestions and recommendations drawn from these studies for practical use.

This study uses the vignettes adapted from D'Arcy et al.'s [70] work since they have been carefully designed and adapted from previous literature to form a non-intrusive way of data collection. These vignettes illustrate situations that require relatively low to moderate levels of malicious intention and computer skills. They offer reasonably realistic and familiar settings that could result in improved internal validity. However, future work using vignettes that illustrate a higher intensity of maliciousness and require more sophisticated computer skills is encouraged.

Additionally, this paper links the vignettes with predictor variables derived from the TPB that have been used to predict intention in many areas related to dysfunctional behaviors. This approach provides an overall reasonable connection between the vignettes and the variables. The usage of scales for the construct items also allows the respondents to

give a lower score to items that may feel disconnected to a certain vignette. Nonetheless, future work using other vignettes and/or variables that are more strongly connected is also encouraged.

As a final point, the respondents in this study are middle managers of medium sized enterprises in Malaysia, and therefore the generalizability of the findings should be treated cautiously as a limitation. Future work with different groups of respondents is strongly recommended.

Acknowledgement

We would like to extend our appreciation to the Associate Editor and the three anonymous reviewers for their insightful comments during the development of the paper. Thanks are also due to Professor Malcolm Smith of University of South Australia for his valuable insights, and to Mr Rudy Adrie Idris, Consul/Education Attaché of Malaysian Consulate-General in Perth, for his kind assistance.

References

[1] Q. Hu, T. Dinev, P. Hart, D. Cooke, Managing employee compliance with information security policies: The critical role of top management and organizational culture, Decision Sciences, 43 (2012) 615-660.
[2] A. Vance, P.B. Lowry, D. Eggett, Using accountability to reduce access policy violations in information systems, Journal of Management Information Systems, 29 (2013) 263-290.
[3] A. Vance, P.B. Lowry, D. Eggett, A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface, MIS Quarterly, (in press).
[4] M. Warkentin, R. Willison, Behavioral and policy issues in information systems security: The insider threat, European Journal of Information Systems, 18 (2009) 101-105.
[5] A. Tsohou, M. Karyda, S. Kokolakis, E. Kiountouzis, Managing the introduction of information security awareness programmes in organisations, European Journal of Information Systems, 24 (2015) 38-58.
[6] R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, R. Baskerville, Future directions for behavioral information security research, Computers & Security, 32 (2013) 90-101.

[7] R. Willison, M. Warkentin, Beyond deterrence: An expanded view of employee computer abuse, MIS Quarterly, 37 (2013) 1-20.
[8] W. Baker, A. Hutton, C.D. Hylender, J. Pamula, C. Porter, M. Spitler, 2011 Data Breach Investigations Report, in, Verizon, 2011.
[9] R. Richardson, 2010/2011 CSI Computer Crime and Security Survey, in, Computer Security Institute, 2011.
[10] S.R. Boss, L.J. Kirsch, I. Angermeier, R.A. Shingler, R.W. Boss, If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security, European Journal of Information Systems, 18 (2009) 151-164.
[11] L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory, Computers & Security, 39, Part B (2013) 447-459.
[12] G.J. Grant, Ascertaining the relationship between security awareness and the security behavior of individuals, in, Nova Southeastern University, United States -- Florida, 2010.
[13] J. Hsu, S.-P. Shih, Y.W. Hung, P.B. Lowry, How extra-role behaviors can improve information security policy effectiveness, Information Systems Research, (in press).
[14] P. Ifinedo, Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition, Information & Management, 51 (2014) 69-79.
[15] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, A. Vance, What levels of moral reasoning and values explain adherence to information security rules? An empirical study, European Journal of Information Systems, 18 (2009) 126-139.
[16] Q. Hu, Z. Xu, T. Dinev, H. Ling, Does deterrence work in reducing information security policy abuse by employees?, Communications of the ACM, 54 (2011) 54-60.
[17] Y. Lee, K.R. Larsen, Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software, European Journal of Information Systems, 18 (2009) 177-187.
[18] N.S. Safa, N.A. Ghani, T. Herawan, Information security conscious care behaviour formation in organizations, Computers & Security, in press (2015).
[19] M. Siponen, M. Adam Mahmood, S. Pahnila, Employees' adherence to information security policies: An exploratory field study, Information & Management, 51 (2014) 217-224.
[20] A. Vance, M. Siponen, S. Pahnila, Motivating IS security compliance: Insights from habit and protection motivation theory, Information & Management, 49 (2012) 190-198.
[21] P. Ifinedo, Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, Computers & Security, 31 (2012) 83-95.
[22] P.B. Lowry, G.D. Moody, Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies, Information Systems Journal, (in press).
[23] J.-Y. Son, Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies, Information & Management, 48 (2011) 296-302.
[24] J. Shropshire, M. Warkentin, S. Sharma, Personality, attitudes, and intentions: Predicting initial adoption of information security behavior, Computers & Security, 49 (2015) 177-191.
[25] J.P. D'Arcy, A. Hovav, Does one size fit all? Examining the differential effects of IS security countermeasures, Journal of Business Ethics, 89 (2009) 59-71.
[26] Y. Baruch, Bullying on the net: Adverse behavior on e-mail and its impact, Information & Management, 42 (2005) 361-371.

[27] J. Glassman, M. Prosch, B.B.M. Shao, To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure, Information & Management, 52 (2015) 170-182.
[28] A. Hovav, J. D'Arcy, Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea, Information & Management, 49 (2012) 99-110.
[29] G.D. Moody, M. Siponen, Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work, Information & Management, 50 (2013) 322-335.
[30] M. Siponen, A. Vance, R. Willison, New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs, Information & Management, 49 (2012) 334-341.
[31] R. Willison, J. Backhouse, Opportunities for computer crime: considering systems risk from a criminological perspective, European Journal of Information Systems, 15 (2006) 403-414.
[32] P.B. Lowry, C. Posey, B. Bennett, T. Roberts, Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational Information Systems Journal, (in press).
[33] P.B. Lowry, C. Posey, T. Roberts, R. Bennett, Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse, Journal of Business Ethics, 121 (2014) 385-401.
[34] C. Posey, R.J. Bennett, T.L. Roberts, Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes, Computers & Security, 30 (2011) 486-497.
[35] C.E. Burns, The relationship between personality and computer deviance, in, Walden University, Ann Arbor, 2013, pp. 124.
[36] C. Posey, T.L. Roberts, P.B. Lowry, R.J. Bennett, J.F. Courtney, Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors, MIS Quarterly, 37 (2013) 1189-1210.
[37] K.H. Guo, Security-related behavior in using information systems in the workplace: A review and synthesis, Computers & Security, 32 (2013) 242-251.
[38] J.P. D'Arcy, T. Herath, A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings, European Journal of Information Systems, 20 (2011) 643-658.
[39] J.M. Stanton, K.R. Stam, P. Mastrangelo, J. Jolton, Analysis of end user security behaviors, Computers & Security, 24 (2005) 124-133.
[40] R.A. Davis, A cognitive-behavioral model of pathological Internet use, Computers in Human Behavior, 17 (2001) 187-195.
[41] G.B. Magklaras, S.M. Furnell, A preliminary model of end user sophistication for insider threat prediction in IT systems, Computers & Security, 24 (2005) 371-380.
[42] I. Ajzen, The theory of planned behavior, Organizational Behavior and Human Decision Processes, 50 (1991) 179-211.
[43] I. Ajzen, T.J. Madden, Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control, Journal of Experimental Social Psychology, 22 (1986) 453-474.
[44] M.K. Chang, Predicting unethical behavior: A comparison of the theory of reasoned action on the theory of planned behavior, Journal of Business Ethics, 17 (1998) 1825-1834.

[45] V. Venkatesh, M.G. Morris, B.D. Gordon, F.D. Davis, User acceptance of information technology: Toward a unified view, MIS Quarterly, 27 (2003) 425-478.
[46] M. Workman, Expert decision support system use, disuse, and misuse: A study using the theory of planned behavior, Computers in Human Behavior, 21 (2005) 211-231.
[47] S.J. Blanke, A study of the contributions of attitude, computer security policy awareness, and computer self-efficacy to the employees' computer abuse intention in business environments, in, Nova Southeastern University, Ann Arbor, 2008, pp. 104.
[48] Y. Cheolho, K. Hyungon, Understanding computer security behavioral intention in the workplace, Information Technology & People, 26 (2013) 401-419.
[49] A. d'Astous, C. François, D. Montpetit, Music piracy on the web - How effective are anti-piracy arguments? Evidence from the theory of planned behaviour, Journal of Consumer Policy, 28 (2005) 289-310.
[50] S.J. Harrington, The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions, MIS Quarterly, 20 (1996) 257-278.
[51] S. Chatterjee, Unethical behavior using information technology, in, Washington State University, United States -- Washington, 2008, pp. n/a.
[52] I. Ajzen, Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior, Journal of Applied Social Psychology, 32 (2002) 665-683.
[53] I. Ajzen, Martin Fishbein's legacy: The reasoned action approach, The ANNALS of the American Academy of Political and Social Science, 640 (2012) 11-27.
[54] T. Hansen, J.M. Jensen, H.S. Solgaard, Predicting online grocery buying intention: A comparison of the theory of reasoned action and the theory of planned behavior, International Journal of Information Management, 24 (2004) 539-550.
[55] N.L. Jimmieson, M. Peach, K.M. White, Utilizing the theory of planned behavior to inform change management: An investigation of employee intentions to support organizational change, Journal of Applied Behavioral Science, 44 (2008) 237 - 262.
[56] Z. Yan, K.-f. Sin, Inclusive education: teachers' intentions and behaviour analysed from the viewpoint of the theory of planned behaviour, International Journal of Inclusive Education, 18 (2013) 72-85.
[57] D.J. Terry, M.A. Hogg, K.M. White, The theory of planned behaviour: Self-identity, social identity and group norms, British Journal of Social Psychology, 38 (1999) 225-244.
[58] M. Workman, An empirical study of a behavioral decision model with moderated effects for long-range security initiatives, Security Journal, 26 (2013) 16-32.
[59] C.J. Armitage, M. Conner, Efficacy of the theory of planned behaviour: A meta-analytic review, The British Journal of Social Psychology, 40 (2001) 471-499.
[60] K. Celuch, S. Goodwin, S.A. Taylor, Understanding small scale industrial user internet purchase and information management intentions: A test of two attitude models, Industrial Marketing Management, 36 (2007) 109-120.
[61] M.B. Curtis, E.A. Payne, An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing, International Journal of Accounting Information Systems, 9 (2008) 104-121.
[62] N. Heinze, Q. Hu, Why college undergraduates choose IT: A multi-theoretical perspective, European Journal of Information Systems, 18 (2009) 462-475.
[63] T.G. Kim, S. Hornung, D.M. Rousseau, Change-supportive employee behavior: Antecedents and the moderating role of time, Journal of Management, 37 (2011) 1664-1693.
[64] F.D. Davis, User acceptance of information technology: System characteristics, user perceptions and behavioral impacts, International Journal of Man-Machine Studies, 38 (1993) 475-487.

[65] E.M. Rogers, Diffusion of Innovations, 5 ed., Simon & Schuster Ltd, London, 2003.
[66] R.L. Thompson, C.A. Higgins, J.M. Howell, Personal computing: Toward a conceptual model of utilization, MIS Quarterly, 15 (1991) 125-143.
[67] J. Wang, M. Gupta, H.R. Rao, Insider threats in a financial institution: Analysis of attack-proneness of information systems applications, MIS Quarterly, 39 (2015) 91-112.
[68] S. Kraemer, P. Carayon, J. Clem, Human and organizational factors in computer and information security: Pathways to vulnerabilities, Computers & Security, 28 (2009) 509-520.
[69] D.R. Dalton, W.D. Todor, Turnover, transfer, absenteeism: An interdependent perspective, Journal of Management, 19 (1993) 193-219.
[70] J.P. D'Arcy, Misuse of Information Systems : The Impact of Security Countermeasures, LFB Scholarly Publishing LLC, New York, NY, USA, 2007.
[71] C. Atzmüller, P.M. Steiner, Experimental vignette studies in survey research, Methodology: European Journal of Research Methods for the Behavioral and Social Sciences, 6 (2010) 128-138.
[72] R. Hughes, M. Huby, The application of vignettes in social and nursing research, Journal of Advanced Nursing, 37 (2002) 382-386.
[73] N.E. Schoenberg, H. Ravdal, Using vignettes in awareness and attitudinal research, International Journal of Social Research Methodology, 3 (2000) 63-74.
[74] K.D. Wason, M.J. Polonsky, M.R. Hyman, Designing Vignette Studies in Marketing, Australasian Marketing Journal (AMJ), 10 (2002) 41-58.
[75] N. Rahman, Caregiver's sensitivity to conflict: The use of vignette methodology, Journal of Elder Abuse and Neglect, 8 (1996) 35-47.
[76] F.N. Kerlinger, Foundations of Behavioural Research, Harcourt Brace, New York, 1992.
[77] J. Pratt, P. Beaulieu, Organizational culture in public accounting: Size, technology, rank, and functional area, Accounting, Organizations and Society, 17 (1992) 667-684.
[78] J.J.v. Muijen, P. Koopman, K.D. Witte, G.D. Cock, Z. Susanj, C. Lemoine, D. Bourantas, N. Papalexandris, I. Branyicski, E. Spaltro, J. Jesuino, J.G.D. Neves, H. Pitariu, E. Konrad, J. Peiró, V. González-Romá, D. Turnipseed, Organizational culture: The focus questionnaire, European Journal of Work and Organizational Psychology, 8 (1999) 551-568.
[79] J.F. Dent, Accounting and organizational cultures: A field study of the emergence of a new organizational reality, Accounting, Organizations and Society, 16 (1991) 705-732.
[80] J. Brick, G. Kalton, Handling missing data in survey research, Statistical Methods in Medical Research, 5 (1996) 215-238.
[81] E. Karanja, J. Zaveri, A. Ahmed, How do MIS researchers handle missing data in survey-based research: A content analysis approach, International Journal of Information Management, 33 (2013) 734-751.
[82] Y. Baruch, B.C. Holtom, Survey response rate levels and trends in organizational research, Human Relations, 61 (2008) 1139-1160.
[83] H.H. Bye, J.G. Horverak, G.M. Sandal, D.L. Sam, F.J. van de Vijver, Cultural fit and ethnic background in the job interview, International Journal of Cross Cultural Management, 14 (2014) 7-26.
[84] J.F. Hair, C.M. Ringle, M. Sarstedt, PLS-SEM: Indeed a silver bullet, Journal of Marketing Theory and Practice, 19 (2011) 139-151.
[85] M. Sarstedt, C.M. Ringle, J.F. Hair, PLS-SEM: Looking back and moving forward, Long Range Planning, 47 (2014) 132-137.
[86] P.B. Lowry, J. Gaskin, Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it, IEEE Transactions on Professional Communication, , 57 (2014) 123-146.

[87] W.W. Chin, Issues and opinion on structural equation modeling, MIS Quarterly, 22 (1998) VII-XVI.
[88] C. Fornell, F. Bookstein, Two structural equation models: LISREL and PLS applied to consumer exit-voice theory, Journal of Marketing Research, 19 (1982) 440-452.
[89] J.F. Hair Jr, M. Sarstedt, L. Hopkins, V.G. Kuppelwieser, Partial least squares structural equation modeling (PLS-SEM), European Business Review, 26 (2014) 106-121.
[90] E.E. Rigdon, Rethinking partial least squares path modeling: In praise of simple methods, Long Range Planning, 45 (2012) 341-358.
[91] P. Bobko, Correlation and Regression, SAGE Publications, Inc., Thousand Oaks, CA, 2001.
[92] N. Kock, WarpPLS 4.0 User Manual, ScriptWarp Systems, Loredo, Texas, 2013.
[93] V.E. Vinzi, L. Trinchera, S. Amato, PLS path modeling: From foundations to recent developments and open issues for model assessment and improvement, in: V.E. Vinzi, W.W. Chin, J. Henseler, H. Wang (Eds.) Handbook of partial least squares: Concepts, methods and applications, Springer Berlin Heidelberg, 2010, pp. 47-82.
[94] J.C. Anderson, D.W. Gerbing, Structural equation modeling in practice: A review and recommended two-step approach, Psychological Bulletin, 103 (1988) 411-423.
[95] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, Multivariate data analysis, 7 ed., Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2010.
[96] D. Gefen, D. Straub, A practical guide to factorial validity using PLS-graph: Tutorial and annotated example, Communications of the Association for Information Systems, 16 (2005) 91-109.
[97] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research, 18 (1981) 39.
[98] J.C. Nunnally, I.H. Bernstein, Psychometric Theory, McGraw Hill, New York, 1994.
[99] N. Urbach, F. Ahlemann, Structural equation modeling in information systems research using partial least squares, Journal of Information Technology Theory and Application, 11 (2010) 5-40.
[100] N. Kock, G.S. Lynn, Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations, Journal of the Association for Information Systems, 13 (2012) 546-580.
[101] T. Coltman, T.M. Devinney, D.F. Midgley, S. Veniak, Formative versus reflective measurement models: Two applications of formative measurement, Journal of Business Research, 61 (2008) 1250-1262.
[102] S. Geisser, The predictive sample reuse method with applications, Journal of the American Statistical Association, 70 (1975) 320-328.
[103] M. Stone, Cross-validatory choice and assessment of statistical predictions, Journal of the Royal Statistical Society. Series B (Methodological), 36 (1974) 111-147.
[104] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, 2nd ed., Lawrence Erlbaum Associates, Hillsdale, New Jersey, 1988.
[105] G. Greene, J.P. D'Arcy, Assessing the impact of security culture and the employee-organisation relationship on IS security compliance, in: 5th Annual Symposium on Information Assurance 2010, New York, 2010.
[106] P. Allen, K. Bennett, PASW Statistics by SPSS: A Practical Guide, version 18.0, 1 ed., Cengage Learning Australia Pty Limited, Sydney, 2010.
[107] D. Lacey, Understanding and transforming organizational security culture, Information Management & Computer Security, 18 (2010) 4-13.
[108] J. Leach, Improving user security behaviour, Computers & Security, 22 (2003) 685-692.

[109] M. Wolf, D. Haworth, L. Pietron, Measuring an information security awareness program, The Review of Business Information Systems, 15 (2011) 9-21.
[110] G. Bloor, P. Dawson, Understanding professional culture in organizational context, Organization Studies, 15 (1994) 275-295.
[111] R.B. Cooper, The inertial impact of culture on IT implementation, Information & Management, 27 (1994) 17-31.
[112] S.A. Herbst, R. Houmanfar, Psychological approaches to values in organizations and organizational behavior management, Journal of Organizational Behavior Management, 29 (2009) 47-68.
[113] B. Kidwell, R.D. Jewell, An examination of perceived behavioral control: Internal and external influences on intention, Psychology and Marketing, 20 (2003) 625-642.

Appendices

Appendix A: Studies on insider dysfunctional behaviors

Behavior themes	**No. of vignettes**	**Behaviors / behavioral intentions studied**	**Stanton et al.'s** [39] **classifications**
Security compliance [10]	0	Keeping up-to-date with latest security threats	Basic hygiene
Security non-compliance [11]	4	Workstation logout	Basic hygiene
		Sharing password	Naïve mistake
		Reading confidential files	Naïve mistake
		Copying organization's sensitive data	Detrimental misuse
Security compliance [12]	0	Locking screen	Basic hygiene
		Participating in security training	Aware assurance
		Alerting virus infection	Aware assurance
		Scanning email attachment	Aware assurance
		Using password autofill features	Naïve mistake
		Sharing computer access	Naïve mistake
		Downloading items from internet	Naïve mistake
Security compliance [17]	0	Adoption of anti-malware	Basic hygiene
Security compliance [18]	0	Information security conscious care	Basic hygiene
Security compliance [21]	0	Intention to comply with information system security policy	Basic hygiene
Security compliance [23]	0	Regular scan for viruses	Basic hygiene
		Compliance with security policy with regards to email	Basic hygiene
		Compliance with security policy with regards to use of internet and network	Basic hygiene
		Installations of operating system patches to prevent unauthorised access	Aware assurance
Security compliance [24]	0	Intention to adopt security software	Basic hygiene
Security non-compliance [15]	1	Password sharing	Naïve mistake

Security non-compliance [16]	3	Unauthorised access (payroll data)	Detrimental misuse
		Unauthorised access and transfer of data	Detrimental misuse
		Stealing and selling confidential data to competitor	Detrimental misuse
Security non-compliance [20]	6	Reading confidential documents	Naïve mistake
		Failing to report computer virus	Naïve mistake
		Allowing children to play with a company laptop	Naïve mistake
		Using unencrypted portable media	Naïve mistake
		Failure to lock (log off) PC	Naïve mistake
		Sharing passwords	Naïve mistake
Information system misuse [25]	2	Unauthorised access	Detrimental misuse
		Unauthorised data modification	Intentional destruction
Information system misuse [26]	0	Cyber bullying	Detrimental misuse
Information system misuse [27]	0	Cyber loafing	Naïve mistake
Information system misuse [28]	4	Unauthorised software installation	Dangerous tinkering
		Email misuse	Detrimental misuse
		Unauthorised access via found password	Detrimental misuse
		Unauthorised record change	Intentional destruction
Information system misuse [29]	0	Using the internet for non-work related activities	Naïve mistake
Information system misuse [35]	0	41 behaviors ranging from non-work related web browsing to sabotage	Cover the following classifications: Dangerous tinkering Detrimental misuse Intentional destruction
Computer abuse [32]	0	10 behaviors ranging from simple non-compliance to physically damaging action	Cover the following classifications: Naïve mistake Dangerous tinkering Detrimental misuse Intentional destruction

Appendix B: Latent constructs' items

Latent constructs	Items
Intention [45, 51]	int1: I intend to carry out a similar action in future. int2: I predict I would carry out a similar action in future. int3: I plan to carry out a similar action in future. int4: If you are in X's situation, how likely is it that you would perform a similar action? int5: All things considered, would you take the same action as X did?
Attitude [45, 51]	att1: Carrying out such action is good. att2: Carrying out such action is valuable.
Subjective norms [42, 45, 51]	sn1: People who influence my behavior think that I should carry out such action. sn2: People who are important to me think that I should carry out such action. sn3: My fellow colleagues would themselves have carried out this action if they had been in my place.
Perceived behavioral control over outcomes (PBC-Out) [45, 66]	Pbc2: Carrying out such action can significantly increase the quality of output of my job. Pbc3: Carrying out such action can significantly increase the quantity of output of my job.
Perceived behavioral control over resources (PBC-Res) [42, 45]	Pbc1: Carrying out such action can decrease the time needed for my important job responsibilities. Pbc4: I have the resources necessary to carry out such action. Pbc5: I have control over carrying out such action.
Organizational culture: Support dimension [78]	In regard to the support in your organization, how many people... Spp1: with personal problems are helped? Spp2: who wish to advance in promotion are supported by their superiors? In regard to the support in your organization, how often... Spp3: is constructive criticism accepted? Spp4: do managers express concern about employees' personal problems? Spp5: are new ideas about work organization encouraged? Spp6: do management practices allow freedom in work?
Organizational culture: Innovation dimension [78]	In regard to the innovation in your organization, how often... inv1: does your organization search for new markets for existing products? inv2: is there a lot of investment in new products? inv3: do unpredictable elements in the market environment present

	good opportunities? inv4: does the organization search for new opportunities in the external environment? inv5: does the company make the best use of the employee skills to develop better products /services? inv6: does the organization search for new products/services?
Organizational culture: Practice dimension [78]	In regard to the practices in your organization, how often... prc1: are instructions written down? prc2: are jobs performed according to defined procedures? prc3: does management follow the rules themselves?
Organizational culture: Performance dimension [78]	In regard to the goal / performance of employees in your organization, how often... pfm1: is competitiveness in relation to other organizations measured? pfm2: is individual appraisal directly related to the attainment of goals? pfm3: does management specify the targets to be attained? pfm4: is it clear how performance will be evaluated? pfm5: are there hard criteria against which job performance is measured? pfm6: is reward dependent on performance?

Appendix C: Vignettes

Vignette 1
Theme: Unauthorized modification
Behavior type: Intentional destruction
Hashim prepares payroll records for the company's employees and therefore has a good access to the timekeeping and payroll system. He periodically changes the amount of hours-worked record of other fellow friends of him by rounding up their total overtime hours such as 39.5 hours to 40 hours

Vignette 2
Theme: Unauthorized access
Behavior type: Detrimental misuse
By chance, Catherine discovered a password that allowed her to access a restricted area of the payroll system of the company. This allowed her to see the salary paid to other employees. At the same time, she was preparing to ask for a raise. Prior to meeting with the management, she accessed and viewed the salaries of others in similar a position to hers. She used this information to determine how much increment to ask for.

Vignette 3
Theme: Unauthorized software installation
Behavior type: Dangerous tinkering
Lee is given a laptop by the company that he can use while in the office as well as on the move. However, the laptop does not have software that allows him to tap into the production planning system that he is authorised to access through other computer terminals. He believes that software will make his work more efficient and effective. A request to the IT department to purchase the software is denied because it is too expensive. To solve the problem, Lee obtains an unlicensed copy of the software and personally installed into the laptop.

Vignette 4
Theme: Unauthorized password sharing
Behavior type: Naïve mistake
Linda works in the marketing department and therefore has access to the company's customer account database. One day at the office, Linda's co-worker in the same department asked to borrow her password in order to access the customer database because she forgot her password. The system administrator who was in charge in resetting the password was on sick leave. Linda gave her password to the co-worker for her to access the customer account database.

Appendix D: t-test for equality of means between mail-based and email-based surveys

Item	T	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
spp1	-0.135	385	0.893	-0.021	0.157
spp2	-1.211	385	0.227	-0.188	0.155
spp3	0.674	385	0.501	0.106	0.157
spp4	0.210	385	0.834	0.034	0.163
spp5	-0.969	385	0.333	-0.141	0.145
spp6	-0.189	385	0.850	-0.032	0.171
inv1	-2.316	385	0.121	-0.381	0.164
inv2	-2.025	385	0.144	-0.319	0.157
inv3	-1.616	385	0.107	-0.229	0.142
inv4	-2.571	385	0.111	-0.385	0.150
inv5	-0.053	385	0.957	-0.009	0.166
inv6	-3.214	385	0.101	-0.570	0.177
prc1	-0.073	385	0.942	-0.011	0.150
prc2	1.618	385	0.106	0.219	0.135
prc3	1.046	385	0.296	0.157	0.150
pfm1	0.635	385	0.526	0.094	0.147
pfm2	0.609	385	0.543	0.086	0.141
pfm3	-0.563	385	0.574	-0.078	0.138
pfm4	1.500	385	0.135	0.241	0.161
pfm5	0.145	385	0.884	0.022	0.149
pfm6	0.590	385	0.556	0.104	0.175
cpx1	-1.262	385	0.208	-0.140	0.111
cpx2	-1.428	385	0.154	-0.200	0.140
cpx3i	-3.218	385	0.101	-0.641	0.199
cpx4i	-4.209	385	0.100	-0.826	0.196
int1	0.708	385	0.479	0.161	0.227
int2	0.096	385	0.924	0.022	0.226
int3	1.681	385	0.094	0.397	0.236
int4	-0.479	385	0.632	-0.115	0.241
int5	-0.462	385	0.644	-0.113	0.244
att1	1.724	385	0.086	0.400	0.232
att2	0.691	385	0.490	0.158	0.228
sn1	2.115	385	0.135	0.469	0.222
sn2	2.167	385	0.131	0.490	0.226
sn3	1.576	385	0.116	0.332	0.211
pbc1	1.624	385	0.105	0.357	0.220
pbc2	0.146	385	0.884	0.032	0.218
pbc3	0.982	385	0.327	0.204	0.208
pbc4	1.542	385	0.124	0.351	0.228
pbc5	1.186	385	0.236	0.273	0.230

Appendix E: Item loadings and crossloadings

	Latent constructs							
Items	ATT	SN	PBC-Out	PBC-Res	INTENT	CULTURE	SE	*p*- value
att1	**0.975**	0.020	0.004	-0.038	-0.023	-0.024	0.044	< 0.001
att2	**0.975**	-0.020	-0.004	0.038	0.023	0.024	0.044	< 0.001
sn1	0.027	**0.967**	-0.070	0.056	0.016	0.002	0.044	< 0.001
sn2	0.080	**0.972**	0.009	-0.060	-0.107	-0.001	0.044	< 0.001
sn3	-0.112	**0.922**	0.064	0.005	0.096	-0.001	0.044	< 0.001
pbc1b	0.052	-0.002	**0.980**	-0.002	-0.028	-0.011	0.044	< 0.001
pbc2b	-0.052	0.002	**0.980**	0.002	0.028	0.011	0.044	< 0.001
pbc1a	-0.034	-0.154	0.114	**0.800**	0.110	0.073	0.044	< 0.001
pbc2a	0.067	0.040	-0.185	**0.917**	-0.042	-0.042	0.044	< 0.001
pbc3a	-0.038	0.097	-0.449	**0.895**	-0.055	-0.022	0.044	< 0.001
int1	0.206	-0.024	-0.036	0.053	**0.947**	0.006	0.044	< 0.001
int2	0.170	.018	0.009	0.007	**0.953**	-0.038	0.044	< 0.001
int3	0.114	0.151	0.104	-0.102	**0.928**	-0.045	0.044	< 0.001
int4	-0.347	-0.044	-0.067	0.004	**0.888**	0.042	0.044	< 0.001
int5	-0.171	-0.105	-0.013	0.039	**0.901**	0.039	0.044	< 0.001
Support	-0.016	0.247	-0.231	0.064	0.000	**0.766**	0.044	< 0.001
Innovation	0.015	-0.051	0.031	0.103	0.030	**0.787**	0.044	< 0.001
Practice	0.188	-0.237	0.265	-0.304	-0.114	**0.796**	0.044	< 0.001
Performance	-0.174	0.047	-0.068	0.130	0.078	**0.857**	0.044	< 0.001

SE = Standard error