Turkish Journal of Computer and Mathematics Education Vol. 12 No.14(2021), 5826-5843
Research Article

Determinants of Protection Intentions Towards Bring Your Own Device Protection Behaviours: A Content Validity Study

Ibrahim Alharthy[1,*], Nor'ashikin Ali[2]

[1]College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia

[2]College of Graduate Studies, Universiti Tenaga Nasional, Malaysia

Article History: *Do not touch during review process(xxxx)*

Abstract: Content validity assessment is an essential step in the instruments development process. Despite its importance,it is an overlookedaspect and is rarely addressed in validating content of the survey instruments forBring Your Own Device (BYOD) protection behaviours. In particular, there is still a lack of systematic approach in conducting a content validity study. The purpose of this article is to demonstrate the procedures in conducting a content validity including preparation of content validation form, selection of experts, reviewing the items, and analysis of the responses from the experts. The content validity for this study relies on expert judgements, who need to provide the evaluation for each item for respective construct in the questionnaire. Their responses were evaluated using Lawshe's technique that uses the calculation of Content Validity Ratio (CVR). The results of CVR showed that 68 questionnaire items are valid for the assessment of determinants of protection behaviours of BYOD. This study will shed lights on procedures in conducting content validity for both practitioners and researchers in BYOD environment, and hence, can improve instruments validity.

Keywords: Content Validity, CVR, BYOD, Protection Behaviour,Lawshe's Technique

1. Introduction

Examining the determinants of bring-your-own-device (BYOD) protection behaviours requires rigorous instruments development. Although the existing scales are available, there is still a lack of instruments with substantial evidence of content validity currently available in BYOD studies. Researchers following rigorous scale development procedures are expected to conduct scale's reliability and validity. The content validity is to ensure that the scales are valid and reliable as well as they should be clear, and easy to administer.Furthermore, the scalesthat are not clear, or excessively long may lower down the response rate, or produce inaccurate response [1]. Without reliable and valid measure, results may be invalid and questionable. Although content validity approach is commonly adopted in case of new instrument development, it is also needed for assessing the validity of existing scales in order to examine any new object[4].Good content validity contributes to the soundness of constructs used in the research; it plays an important role in the development of instruments, and therefore, it should be conducted rigorously. Content validity is an essential step in the survey instrument's development, and is used as a tool to verify one's instruments as it assures that constructs are drawn from the theoretical essence of what they propose to measure; hence, it should be given a priority in instruments development stages[11].Gable[2] contended that "content validation should receive the highest priority during the process of instrument development" (p.72). Furthermore, it is an essential step to be completed prior to assessing other types of validity.David et al.[3]identified five sources of validity evidence: the content, response process, internal structure, relation to other constructs, and consequence. Despite various definitions of content validity emerged since decades ago, the general definition of validity refers to the extent to which the instrument measures what it intends to measure[5].Content validity provides evidence about the degree to which items or measures of instrument adequately reflect the construct operational definition.A construct refers to the concept, attribute, or variable that one wishes to measure using survey questions. Content validity involves the evaluation of all aspects of the measurement process including questionnaire items, response formats, and instructions.

Theissue of content validity has been controversial, and attempts were made to establish methods for determining content validity. For example, Schmitz and Storey [4]assessed content validity using an iterative pre-study process (wash, rinse, and repeat until clean), whileotherstudies reported achieving content validity through a review of literature[5]. Years ago, some researchers established methods to quantify the process [5,6,7]by conducting a quantitative assessment with a group of subject matter experts (SMEs)with the argument thatthe knowledge of the content domain resides in the heads of subject matter experts (SMEs). Hence, the opinions of subject matter experts in the content validity process may provide useful insights into the completeness and appropriateness of the items[8]. It is argued that subject matter experts' judgment is important to justify the content validity of the instruments. In line with this[9,10] determined a validity assessment using content validity index (CVI) to validate the relevance of items using subject-matter experts, who rated items for their relevance. Previous BYOD studies[11, 12] did not establish any procedures for content validity assessment.

In instruments development process for exploring the determinants of BYOD protection behaviours, establishing content validity is an important step to support the validity of a questionnaire, which is a measurement tool used in this research[13]. Most of the measurement items used in this study were taken from previous studies, and adopted in BYOD context. Thus, assessing the validity of existing scales is needed in order to examine constructs from BYOD perspective.This study aims to establish the procedures for assessing the content validation instruments used to measure the determinants of protection intentions towards bring your own device protection behaviours. This study used Lawshe's technique for screening the items of constructs for achieving content validity[7].Insights gained during this process contributes to the knowledge by demonstrating the importance of content validity and measure development in practice. This study provides guides to researchers in conductinga content validity study for theirinstruments development process. This study outlined the quantitative and qualitative approaches to evaluate content validity. In addition, this study described the criteria for conducting the procedures and presented the model's determinants assessment results. The research model contains twelve constructs (one (1) mediating construct, one (1) dependent constructand ten (10) independent constructs) and has 68 items. Table 1 provides the summary ofthe determinants.

Table 1: Constructs Definition

Abbreviation	Constructs	Definition	Refers
SE	Self-Efficacy	"It is the expectation of individuals' ability to perform the behaviours in terms of achieving desired protection outcomes".	[14],[15]
RE	Response Efficacy	"It is the beliefs of individuals, whether a step of protection would avoid the threat or not".	[16],[15]
PS	Perceived Severity	"It is the perception of individuals to the results of protection from threats".	[14],[15]
PV	Perceived Vulnerability	"An individual's belief in the possibility of a threat or breach due to lack of protection".	[17],[15]
RC	Response Cost	"It is a behavioural procedure that involves the loss of protection by individuals that result in unacceptable behaviour".	[16],[15]
ATT	Attitude	"It is the willingness of individuals to respond positively or negatively to the direction of protection".	[14],[15]
SN	Subjective Norms	"It is a social condition for individuals to perform or not for protection behaviours".	[14],[15]
ISA	Information Security Awareness	"It raises awareness about the potential dangers of rapidly evolving forms of information and the rapidly evolving threats to that information that targets human behaviour".	[14],[15]
SSE	Security Self-Efficacy	"Individuals can minimize information system security threats and protect information system assets from security attacks".	[18],[19]
PBC	Perceived Behavioural Control	"It is the perceptions and intentions of individuals about their ability to protect their data".	[20],[21]
KNOW	Knowledge	"It is the individual's understanding and utilization of information technology and their level of knowledge to protect their data."	[22],[23]
PI	Protection Intention	"It is the intention of employees to protect the organization's information and technology resources from potential security leakages".	[24],[25]
PB	Protection Behaviour	"It is the behaviour of employees to protect the information and technology resources of the organization from potential security leakages."	[26],[27]

2. Content Validation Procedures

This study follows five stages of content validation procedures as presented in Figure 1.

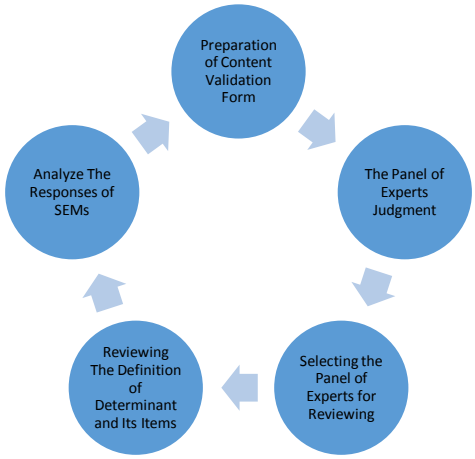

Figure 1: Five Stages of Content Validation Study

2.1 Preparation of Content Validation Form

The initial stage of content validation is to set up content validation to guarantee the expert's review panel has clear expectations and understanding of action. The rating scale and the instructions are mentioned in Figure 2. The suggested rating scale by [28] and [29]has been utilized to score individual items as shown in Figure 3. In addition, a domain is defined as facilitating the experts' scoring process.

QUESTIONNAIRE VALIDATION

Dear Professor/Assoc. Professor/Dr.,

Greeting

I am currently pursuing my PhD study in College of Computing and Informatics at Universiti Tenaga Nasional (Malaysia). My research topic is related to "Determinants of Protection Intentions Towards Bring Your Own Device Protection Behaviours among Employees". I would like to seek your cooperation as a content expert validating my scales before proceeding to the pilot study. The idea behind this validation is to check whether the items are reflecting the operational definition of the study constructs or not. **Appreciated it if you exert time to reviewing the items and evaluate content validity.**

Requesting you to assess each statement of the question based on the criteria in the following details:

Indicator	**Details**
Essential	Maintain item as it is
Important (but not essential)	Maintain item, but needs some redefining
Not Relevant	Remove Item

I also highly appreciate any extra suggestions for the improvement of the content of the questions to enhance the effectiveness of the survey instrument. Kindly don't hesitate to reach me if I may clarify any issue related to the above requirements to the contact details below.

Thank you very much for your valuable feedback, time and cooperation.

Yours sincerely,

Ibrahim Alharthy, Ph.D. Candidate

Figure 2: The Rating Scale and Instruction of the Content Validation Form to the Experts

RE. Response Efficacy:

The response efficacy is defined as the development of individual's intention to abide by relevant policies when using personal devices and affected employees perceived response efficacy in demonstrating BYOD compliance behaviour.

Item		Remarks
RE1	Complying with my personal device security policy reduces the security threat to my organizations information.	
RE2	Complying with my personal device security policy reduces the security threat to my personal data.	
RE3	If I comply with my personal device security policy, my organization's mobile security problems will be scarce.	
RE4	If I comply with my personal device security policy, my mobile device related security problems will be scarce.	
RE5	Compliance with my personal device security policy helps to reduce IS security problems in my organization.	
RE6	Compliance with my personal device security policy helps me reduce security problems with my own personal data.	

Please, recommend any other items that you think are more compatible with measuring the determinant of "Response Efficacy" or any comments on the above-mentioned items I suggested.

Figure 3: The layout form of the content validation, the definition of determinant, items represent (measure) and Content Validate Ratio (CVR).

2.2 The Panel of Experts Judgment

The approaches of qualitative and quantitative were used to survey the expert's judgment [30]. As this study adopted quantitative and qualitative approaches, the panel of experts' judgment is to look at every item relevant to the determinant. The researchers proposed approaches to assess the content validity. Most of those approaches were used to analyze panel expert evaluations' consistency or agreement. Additionally[31,32,33, 34] proposed approaches that involved the experts (SEMs) experts in rating every item (questionnaires) for every determinant (construct) in a conceptual study model. Thus, the decisions about retaining the items and reviewing feedbacks are based on experts (SMEs), who critically review and provide verbal and written comments to improve the suitable items (questionnaires) to the study domain[13].Moreover, the selection of SMEs will impact the validation process sufficiency [35]. Davis and Rubio et al.[1] recommended that expert panels have professional certification in the research area and have work experience in the research scope. According toBahry et al.[10], the study recommended that the required number of experts is at least three. The study of [36] suggested a range between two and twenty experts. Waltz et al.[37] recommended that not less than two reviewers of the research scope are required and evaluators for instrument construction.

2.3 Selecting The Panel of Experts for Reviewing

Following the guidelines [28], [7] and [35], this study selected experts from the area of industry and knowledgeable academia in the content area of information security, information systems and who have a knowledgeable background about the development of survey measurement. Grant et al. [38]recommended not to select the members from one geographic location of researchers' countries. Selecting individuals of (SEMs) from various areas can increase the accuracy of compatible items (questionnaires) and knowledge of experts to a study instrument. This study developed the instruments to test the determinants of protection intentions towards bring your own device protection behaviours. Therefore, it is recommended that experts have the following criteria:

- Have background experience in information security and an idea about BYOD usage.

- Have published papers on the concepts and theories on protection intentions and behaviours.

- Have published papers related to information systems.

2.4 Reviewing The Definition of Determinants and Its Items

This study used an online survey via google form for quick access, and the sample contained experts of several geographic areas. Because of the COVID-19 pandemic, the questionnaire's validation form was sent to the experts through email. Fourteen experts received an email invitation form containing a URL link of the response form and a soft copy of the validation form (MS Word). The email included an introductory letter to request the panel individuals' participation. The introductory letter clarified the purpose of the study and the expert's tasks in the study in which they agreed to participate. The study survey form introduced the guidelines to fill up, and followed the suggestions of [28, 7]to evaluate the measures or constructs using a scale from 1 to 3 where 1 means not relevant, 2 means are important (but not essential), and 3 means essential. The open questions were included to obtain the feedback from SMEs on any other items they think could reflect the constructs. The experts were requested to understand the constructs definition and the measurement items, and then put a score for each item. They were requested to write comments or compose suggestions to improve items' relevance to the designated domain. All suggestions were taken into accountto refine the constructsand the items.

2.5 Analyze The Responses of Experts

Lawshe has developed the content validity ratio (CVR) method to measure an item's validity [7]. The Lawshe technique has propositioned a quantitative evaluation of content validity. It utilizes a panel of SMEs to rate the level to every test item that addresses the target or domain. Based on the methodology used in this study, the SMEs were requested to judge the importance of every constructbased on 3 scale: "1 = not relevant", "2 = important (but not essential)", "3 = essential". The CVR was calculatedbased on the technique developed by [7]:

$$CVR = (2Ne / N) – 1$$

The CVR is standard for Content Validity Ratio, Ne = number of SMEs appearing "essential", and N = whole numbers of SMEs. The CVR outcome is shown inTable 2.

Table 2: The CVR Category

Category	Details	CVR
Essential	When all the experts agreed that it is “essential”	1.00 (100% agreement)
Important (but not essential)	"Essential" is agreed by experts when more than half (> 50%), but less than all (< 100%)	Range (0 and 0.99)
Not Relevant	Then half of the experts (<50%) agreed that it is "essential"	Negative

This study adopted Lawshe's technique as recommended by [28] because it has (when N >= 10) a number of experts. This technique was more straightforward as it uses the experts (SMEs) to select accurate and convenient items (questionnaires) that represent the domain. According to the studies by [7] and [29], the categories of "important (but not essential)" and "essential" by responses must be used because both are the positive indicators of CVR value for items (questionnaires) to a determinant (construct).

Of the total thirty experts who received the survey, only fourteen respondents agreed to participate. From thirteen respondents rated the items, there was one respondent, who suggested comments without rating the items. Therefore, the total number of SMEs, who responded and filled the form was thirteen (N=13). A Content Validity Ratio (CVR) was computed for each item from these respondents' data. The content validity assessment results illustrated that using determinants of protection intentions towards bring your own device protection behaviours model has a high level of acceptance in content validity, and thus, the items (questionnaires) were confirmed as the representation of domain. Table 3 provides a list of all the constructs (determinants), evaluates an overall number of items, and a total number of statistically significant items (questionnaires) according to CVR values in this study and the comments.

Table 3 SMEs' Analysis and Feedback regarding the Constructs (Determinants)

Constructs (Determinants)	Total Items	Significant Items	Comments
Self-Efficacy	6	-	According to SMEs' comments and suggestions, they suggest to usethe determinant of security self-efficacy instead of self-efficacy.
Response Efficacy	6	5	One item will be excluded and will keep the remaining five items.
Perceived Severity	6	6	All six items are essential and important.
Perceived Vulnerability	7	6	One item will be excluded and will keep the remaining six items.
Response Cost	6	6	All six items are essential and important.
Attitude	6	5	One item will be excluded and will keep the remaining five items.
Subjective Norm	6	5	One item will be excluded and will keep the remaining five items.
Perceived Behavioural Control	7	6	One item will be excluded and will keep the remaining six items.
Information Security Awareness	10	8	Two items will be excluded and will keep the remaining eight items.
*Security Self-Efficacy	5	5	All five items are essential and important.
Protection Intention	7	6	One item will be excluded and will keep the remaining six items.
Knowledge	6	6	All six items are essential and important.
Protection Behaviour	4	4	All six items are essential and important.
Total of Items	82	68	
*Indicatesusing the determinant of security self-efficacy instead of self-efficacy			

According to the feedback of the SMEs, below is the list of salient points and suggestions to be considered:

1- Use security self-efficacy rather than self-efficacy. The main focus of this study is security. So, it will use the determinant security self-efficacy and exclude the determinant self-efficacy.
2- Limit each determinant's measures to be a maximum of 5 or 6 items (Questions). If more than 5 or 6 items, the potential participants may find the questionnaire a bit long.
3- Use the measures (items) that focus on its effect on organizations from the employees.
4- Merge some measures (items) to keep the audience more interested in answering a survey.
5- Paraphrasing and proofreading some measures (items).

In this study, the questionnaire was adopted from previous studies. However, SMEs did not feel that some items suggested in this study were applicable in the study context. Therefore, only items recommended by SMEs, and that fulfil CVR valueswill be used in the final survey to be distributed to the participants among Oman government civil employees.

3. Conclusion

This paper soughtto study content validity issues for protection behaviours when using BYOD. Content Validity Ratio (CVR) proposed by Lawshe was used to determine the content validity of the constructs in addition to comments by SMEs.

This study demonstrated that most of the constructs (determinants) have good validity measurement items (68 items out of 82), and thus, can be used for final survey. This study provides insights to researchers and practitioners on the assessment procedures for achieving content validity. Future research should look into replicating this content validity approach to other measurement items.

References

[1] D. M. G. Rubio, M. Berg-Weger, S. S. Tebb, E. S. Lee, and S. Rauch, "Objectifyng content validity: Conducting a content validity study in social work research," *Soc. Work Res.*, vol. 27, no. 2, pp. 94–104, 2003, doi: 10.1093/swr/27.2.94.

[2] Robert K . Gable, "Instrument development in the affective domain," no. 1986, pp. 1–164, 1986.

[3] F. David A. Cook, MD, MHPE, Thomas J. Beckman, MD, "Current concepts in validity and reliability for psychometric instruments: Theory and application," *Am. J. Med.*, vol. 119, no. 2, pp. 166.e7-166.e16, 2006, doi: 10.1016/j.amjmed.2005.10.036.

[4] K. Schmitz and V. C. Storey, "Empirical test guidelines for content validity: Wash, rinse, and repeat until clean," *Commun. Assoc. Inf. Syst.*, vol. 47, no. 1, pp. 787–850, 2020, doi: 10.17705/1CAIS.04736.

[5] D. Abrego Almazán, Y. Sánchez Tovar, and J. M. Medina Quintero, "Influence of information systems on organizational results," *Contaduria y Adm.*, vol. 62, no. 2, pp. 321–338, 2017, doi: 10.1016/j.cya.2017.03.001.

[6] J. Cohen, "Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit," *Psychol. Bull.*, vol. 70, no. 4, pp. 213–220, 1968, doi: 10.1037/h0026256.

[7] C. H. Lawshe, "A quantitative approach to content validity," *Pers. Psychol.*, vol. 28, pp. 563–575, 1975.

[8] Mary R. Lynn, "Determination and Quantificatiom of Conten Validity," *Journal of Experimental Psychology: General*, vol. 35, no. 6. pp. 382–386, 1986, [Online]. Available: http://ijoh.tums.ac.ir/index.php/ijoh/article/view/26.

[9] J. Mason, S. Classen, J. Wersal, and V. P. Sisiopiku, "Establishing face and content validity of a survey to assess users' perceptions of automated vehicles," *Transp. Res. Rec.*, vol. 2674, no. 9, pp. 47–538, 2020, doi: 10.1177/0361198120930225.

[10] F. D. Saiful Bahry, M. Masrom, and M. N. Masrek, "Measuring validity and reliability of website credibility factors in influencing user engagement questionnaire," *Int. J. Web Inf. Syst.*, vol. 17, no. 1, pp. 18–28, 2021, doi: 10.1108/IJWIS-08-2020-0050.

[11] P. Baillette, Y. Barlette, and A. Leclercq-Vandelannoitte, "Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users," *Int. J. Inf. Manage.*, vol. 43, no. July, pp. 76–84, 2018, doi: 10.1016/j.ijinfomgt.2018.07.007.

[12] D. Dang-Pham and S. Pittayachawan, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach," *Comput. Secur.*, vol. 48, pp. 281–297, 2015, doi: 10.1016/j.cose.2014.11.002.

[13] M. S. B. Yusoff, "ABC of Content Validation and Content Validity Index Calculation," *Educ. Med. J.*, vol. 11, no. 2, pp. 49–54, 2019, doi: 10.21315/eimj2019.11.2.6.

[14] Tejaswini Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.

[15] N. Ameen, A. Tarhini, M. H. Shah, N. Madichie, J. Paul, and J. Choudrie, "Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce," *Comput. Human Behav.*, vol. 114, no. April 2020, p. 106531, 2021, doi: 10.1016/j.chb.2020.106531.

[16] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, 2012, doi: 10.1016/j.im.2012.04.002.

[17] F. Putri and A. Hovav, "Employees' compliance with BYOD security policy: Insights from reactance, organizational

justice, and protection motivation theory," *ECIS 2014 Proc. - 22nd Eur. Conf. Inf. Syst.*, pp. 1–17, 2014.

[18] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, 2009, doi: 10.1287/isre.1070.0160.

[19] F. J. Haeussinger and J. J. Kranz, "Information security awareness : its antecedents and mediating efffects on SECURITY COMPLIANT BEHAVIOR," *2013*, pp. 1–16.

[20] Y. Chen, C. Liang, and D. Cai, "Understanding WeChat Users' Behavior of Sharing Social Crisis Information," *Int. J. Hum. Comput. Interact.*, vol. 34, no. 4, pp. 356–366, 2018, doi: 10.1080/10447318.2018.1427826.

[21] L. Zhao, J. Yin, and Y. Song, "An exploration of rumor combating behavior on social media in the context of social crises," *Comput. Human Behav.*, vol. 58, pp. 25–36, 2016, doi: 10.1016/j.chb.2015.11.054.

[22] A. Duke Giwah, "User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2018-April, pp. 1–5, 2018, doi: 10.1109/SECON.2018.8479178.

[23] A. Musarurwa, S. Flowerday, and L. Cilliers, "An information security behavioural model for the bring-your-own-device trend," *SA J. Inf. Manag.*, vol. 20, no. 1, pp. 1–9, 2018, doi: 10.4102/sajim.v20i1.980.

[24] B. S. Chon, J. K. Lee, H. Jeong, J. Park, and J. Park, "Determinants of the Intention to Protect Personal Information among Facebook Users:," *ETRI J.*, vol. 40, no. 1, pp. 146–155, 2018, doi: 10.4218/etrij.2017-0082.

[25] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS," vol. 34, no. 3, pp. 523–548, 2010.

[26] A. Koohang, K. Floyd, N. Rigole, and J. Paliszkiewicz, "Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs," *Online J. Appl. Knowl. Manag.*, vol. 6, no. 2, pp. 7–22, 2018, doi: 10.36965/ojakm.2018.6(2)7-22.

[27] S. Milne, P. Sheeran, and S. Orbell, "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory," *J. Appl. Soc. Psychol.*, vol. 30, no. 1, pp. 106–143, 2000, doi: 10.1111/j.1559-1816.2000.tb02308.x.

[28] N. Ali, A. Tretiakov, and D. Whiddett, "A Content Validity Study for a Knowledge Management System Success Model in Healthcare," *JITTA J. Inf. Technol. Theory Appl.*, vol. 15, no. 2, p. 21, 2014.

[29] B. R. Lewis, G. F. Templeton, and T. A. Byrd, "A methodology for construct development in MIS research," *Eur. J. Inf. Syst.*, vol. 14, no. 4, pp. 388–400, 2005, doi: 10.1057/palgrave.ejis.3000552.

[30] E. S. Haynes, S.N., Richard, D.C.S. & Kubany, "Content validity in psychological assessment: A functional approach to concepts and methods," *The American Psychological Association, Inc.*, vol. Vol. 7, no. No. 3. pp. 238–247, 1995.

[31] S. V. O. Denise F. Polit, Cheryl Tatano Beck, "Is the CVI an Acceptable Indicator of Content Validity? Appraisal and Recommendations," pp. 488–495, 2007, doi: 10.1002/nur.

[32] J. C. Anderson and D. W. Gerbing, "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychol. Bull.*, vol. 103, no. 3, pp. 411–423, 1988, doi: 10.1037/0033-2909.103.3.411.

[33] C. A. Schriesheim, K. J. Powers, T. A. Scandura, C. C. Gardiner, and M. J. Lankau, "Improving Construct Measurement In Management Research: Comments and a Quantitative Approach for Assessing the Theoretical Content Adequacy of Paper-and-Pencil Survey-Type Instruments," vol. 19, no. 2, pp. 385–417, 1993.

[34] T. R. Hinkin and J. B. Tracey, "An Analysis of Variance Approach to Content Validation," *Organ. Res. Methods*, vol. 2, no. 2, pp. 175–186, 1999, doi: 10.1177/109442819922004.

[35] L. L. Davis, "Instrument review: Getting the most from a panel of experts," *Appl. Nurs. Res.*, vol. 5, no. 4, pp. 194–197, 1992, doi: 10.1016/S0897-1897(05)80008-4.

[36] R. K. Gable and M. B. Wolf, "Instrument development in the affective domain: Measuring attitudes and values in corporate and school settings," pp. 1–275, 1993.

[37] C. F. Waltz, O. L. Strickland, and E. R. Lenz, “Measurement in Nursing and Health Research,” *Meas. Nurs. Heal. Res.*, 2005, doi: 10.1891/9780826170620.

[38] C. Grant, J., Kinney, M., & Guzzetta, “A methodology for validating nursing diagnoses. Advances in Nursing.” p. 8, 1990, [Online]. Available: papers://44a5bfc5-03a8-49b9-9f07-1fbfe6b6320a/Paper/p208.

Appendix 1: Summarized the Calculate of the CVR Values and SMEs Comments for Each Determinant

Determinant	Total Items	Significant Items	Essential	Important (but not essential)	Not Relevant	CVR of Items	Select (✓)/ Remove (X) of Items	Comments byExperts
Self-Efficacy	6	**SE1:** I would feel comfortable following most of the security policies on my own personal device.	8	4	1	0.23	✓	According to SMEs' comments and suggestions, they suggest to use the determinant of security self-efficacy instead of self-efficacy
		SE2: If I wanted to, I could easily follow security policies on my own personal device.	8	4	1	0.23	✓	
		SE3: I would be able to follow most of the security policies on my own personal device even if there was no one around to help me.	10	3	-	0.53	✓	
		SE4: I am aware that there are privacy controls when I use my own personal device.	8	4	1	0.23	✓	
		SE5: I understand that there are privacy controls when I use my own personal device.	8	4	1	0.23	✓	
		SE6: I am aware of organization-based settings when I use my own personal device.	8	4	1	0.23	✓	
Response Efficacy	6	**RE1:** Complying with my personal device security policy reduces the security threat to my organizations information.	10	2	1	0.53	✓	RE4 item will be excluded and will keep the remaining five items
		RE2: Complying with my personal device security policy reduces the security threat to my personal data.	12	1	-	0.84	✓	
		RE3: If I comply with my personal device security policy, my organization's mobile security problems will be scarce.	7	3	3	0.07	✓	
		RE4: If I comply with my personal device security policy, my mobile device related security problems will be scarce.	6	5	2	-0.07	**X**	

		RE5: Compliance with my personal device security policy helps to reduce IS security problems in my organization.	8	3	2	0.23	✔	
		RE6: Compliance with my personal device security policy helps me reduce security problems with my own personal data.	8	4	1	0.23	✔	
Perceived Severity	6	**PS1:** If I break information security rules when using my personal device, my organization will discipline me.	10	2	1	0.53	✔	All six items are essential and important.
		PS2: If I repeatedly break security rules when using my personal device, my organization will terminate me.	8	3	2	0.23	✔	
		PS3: If I were caught violating organization information security policies, I would be severely punished.	10	3	-	0.53	✔	
		PS4: I believe that organization information when stored on my personal device will be vulnerable to security incidents.	11	2	-	0.69	✔	
		PS5: I believe an organization's productivity and its employees will be threatened by security incidents when using a personal device.	9	4	-	0.38	✔	
		PS6: I believe the profitability of organisations is threatened by security incidents when using a personal device.	9	3	1	0.38	✔	
Perceived Vulnerability	7	**PV1:** I could be subjected to an information security threat if I don't comply with my own personal device security policy in my organization.	10	3	-	0.53	✔	PV6 item will be excluded and will keep the remaining six items.
		PV2: If I don't comply with security policy when using my personal device, a security problem to my organization's information	9	4	-	0.38	✔	

		could occur.						
		PV3: If I don't comply with the organization's security policy when using my personal device, a security problem to my personal data could occur.	9	2	2	0.38	✓	
		PV4: I know my organization could be vulnerable to security breaches if I don't adhere to it IS policy when using my personal device.	10	2	1	0.53	✓	
		PV5: I could fall victim to a malicious attack if I fail to comply with my organization's IS policy when using my personal device.	12	1	-	0.84	✓	
		PV6: I believe that protecting my company's information will reduce illegal access to it when using my personal device.	6	5	2	-0.07	**X**	
		PV7: If I don't pay adequate attention to guidelines when using my personal device, my organization's data and resources may be compromised.	7	6	-	0.07	✓	
Response Cost	6	**RC1:** Complying with my personal device security policy interferes with my work.	7	2	4	0.07	✓	All six items are essential and important.
		RC2: Complying with personal device security policy interferes with the personal use of my device.	8	2	3	0.23	✓	
		RC3: There are too many overheads associated with complying with personal device security policies.	7	5	1	0.07	✓	
		RC4: Complying with personal device security policy would require a considerable investment of effort other than time.	7	4	2	0.07	✓	
		RC5: Complying with personal device security policy would take a considerable amount of my working time.	9	2	2	0.38	✓	

		RC6: Complying with a personal device security policy would take a considerable amount of my personal time.	7	6	-	0.07	✔	
Attitude	6	**ATT1:** I believe that it is beneficial for an organization to establish clear BYOD security policies, practices, and technologies.	11	1	1	0.69	✔	ATT6 item will be excluded and will keep the remaining five items.
		ATT2: I believe that it is useful for an organization to enforce its BYOD security policies, practices, and technologies.	8	4	1	0.23	✔	
		ATT3: I believe that it is a good idea for an organization to establish clear BYOD security policies, practices, and technologies.	9	1	3	0.38	✔	
		ATT4: If I am aware of my organization's sensitive nature and systems, if managed well, BYOD's advantages outweigh the risks in today's modern technological era.	8	3	2	0.23	✔	
		ATT5: I believe that personal devices are being optimally managed within my organization to maximize their benefits while mitigating information security risks.	7	5	1	0.07	✔	
		ATT6: In light of the nature of my work and industry, the organization should be able to monitor what I do on my personal device while in the work environment.	5	5	3	-0.23	**X**	
Subjective Norms	6	**SN1:** People who are influential to me think that I should follow the policies and procedures and use the security technologies for my personal device.	7	4	2	0.07	✔	SN3 item will be excluded and will keep the remaining five items.
		SN2: I should follow the policies and procedures and use the security technologies for my personal device as people who are important to me think that.	7	4	2	0.07	✔	

		SN3: I respect people who think that I should follow the policies and procedures and use the security technologies for my personal device.	6	3	4	-0.07	**X**	
		SN4: Top management thinks I should follow organizational IS security policies when using my personal device.	9	2	2	0.38	✔	
		SN5: My colleagues think that I should follow organizational IS security policies when using my personal device.	8	3	2	0.23	✔	
		SN6: I should follow organizational IS security policies when using my personal device as my organization's information security department thinks.	7	4	2	0.07	✔	
Perceived Behavioural Control	7	**PBC1:** I think it's easy for me to share organizational information by using my personal device.	7	6	-	0.07	✔	PBC7 item will be excluded and will keep the remaining six items.
		PBC2: I am confident that if I want, I can share organizational information by using my personal device.	7	4	2	0.07	✔	
		PBC3: I have time, resources and knowledge to share organizational information by using my personal device.	8	3	2	0.23	✔	
		PBC4: I believe that information security conscious care behavior is not a problematic practice when using my personal device.	9	4	-	0.38	✔	
		PBC5: I believe that my experiences help me have careful behavior about information security when using my personal device.	8	3	2	0.23	✔	
		PBC6: Following information security policies and procedures is easy for me when using my personal device.	7	4	2	0.07	✔	
		PBC7: Information security conscious care behavior is an achievable practice when using	5	7	1	-0.23	**X**	

		my personal device.						
Information Security Awareness	10	**ISA1:** My organization provides training to help employees improve their awareness of personal device information security issues.	10	3	-	0.53	✓	ISA6 and ISA10 items will be excluded and will keep the remaining eight items.
		ISA2: My organization provides employees with education on personal device software copyright laws.	8	4	1	0.23	✓	
		ISA3: In my organization, employees are briefed on the consequences of modifying BYOD data in an unauthorized way.	9	4	-	0.38	✓	
		ISA4: My organization educates employees on their personal device security responsibilities.	7	4	2	0.07	✓	
		ISA5: In my organization, employees are briefed on the consequences of accessing BYOD that they are not authorized to use.	8	4	1	0.23	✓	
		ISA6: I am aware of the potential security threat when using my personal device.	6	5	2	-0.07	**X**	
		ISA7: I have sufficient knowledge about the cost of information security breaches when using my personal device.	9	3	1	0.38	✓	
		ISA8: I understand the risk of information security incidents when using my personal device.	10	3	-	0.53	✓	
		ISA9: I keep myself updated in terms of information security awareness when using my personal device.	7	5	1	0.07	✓	
		ISA10: I share information security knowledge to increase my awareness when using my personal device.	6	5	2	-0.07	**X**	

Security Self-Efficacy	5	**SSE1:** For me, taking information security precautions to protect my organization's information and information systems is easy when using my personal device.	7	4	2	0.07	✓	All five items are essential and important.
		SSE2: I have the expertise to protect my business and private data when using my personal device.	7	3	3	0.07	✓	
		SSE3: I have the necessary skills to protect my organizations information and information systems from information security violations when using my personal device.	9	4	-	0.38	✓	
		SSE4: My skills required to stop information security violations against my organization's information and information systems are adequate when using my personal device.	7	4	2	0.07	✓	
		SSE5: I believe that I could learn to perform preventive measures to protect my organization's information and information systems effectively when using my personal device.	8	3	2	0.23	✓	
Protection Intention	7	**PI1:** I will set the protection of personal information to maintain privacy during the use of my personal device.	10	3	-	0.53	✓	PI2 item will be excluded and will keep the remaining six items.
		PI2: I will actively monitor whether my information is stolen to protect my private life.	5	5	3	-0.23	**X**	
		PI3: I do not want to disclose personal information when using my personal device.	8	4	1	0.23	✓	
		PI4: I will limit the organization-based information I share when using my personal device.	8	4	1	0.23	✓	
		PI5: I plan to limit the access applications have to organization based information when	8	3	2	0.23	✓	

		using my personal device.						
		PI6: I will likely enable private browsing when using my personal device.	8	3	2	0.23	✔	
		PI7: I will limit the ability of advertisers to track me when using my personal device.	7	5	1	0.07	✔	
Knowledge	6	**KNOW1:** I have sufficient knowledge to protect organization data when using my personal device.	8	3	2	0.23	✔	All six items are essential and important.
		KNOW2: Using a personal device at work would allow me access to all the information I require in order to perform my job satisfactorily.	8	3	2	0.23	✔	
		KNOW3: I have sufficient knowledge to process the protection when using my personal device.	8	4	1	0.23	✔	
		KNOW4: I am well informed about how to deal with problems caused by the organization's data when using my personal device.	8	3	2	0.23	✔	
		KNOW5: There is a growing demand from employees for the use of personal. devices in the organization environment to allow unmonitored access to information and systems.	9	2	2	0.38	✔	
		KNOW6: Organizations that allow employees to bring their own devices are more information security conscious than those that do not.	8	3	2	0.23	✔	
Protection Behaviour	4	**PB1:** I comply with personal devices protection recommendations.	9	3	1	0.38	✔	All four items are essential

		PB2: I do my best to follow personal devices protection rules and procedures strictly.	10	3	-	0.53	✔	and important.
		PB3: I am certain that I will follow organizational, personal device protection recommendations (if they exist).	7	2	4	0.07	✔	
		PB4: My personal device is secured by a password.	8	2	3	0.23	✔	