Competence Measure in Social Networks

Samar Muslah Albladi and George R S Weir
Department of Computer and Information Sciences
University of Strathclyde, UK
{samar.albladi; george.weir}@strath.ac.uk

***Abstract*— The current research aims to gain insight on user competence in detecting security threats in the context of online social networks (OSNs) and investigates the multidimensional space that determines this user competence level. The role of user competence and its dimensions in facilitating the detection of online threats is still a controversial topic in the information security field. The dimensions used to measure the concept are self-efficacy, security awareness, privacy awareness, and cybercrime experience. The scales used to measure those factors can determine the level of user competence in evaluating risks associated with social network usage. The measurement scales employed here have been validated using an item-categorization approach that, to our knowledge, has never before been used in information security research. The result of this study provides evidence for the suitability and validity of the user competence dimensions and associated measurement scales.**

***Keywords*—Information Security, Privacy Awareness, Security Awareness, Social Network, User Competence.**

I. INTRODUCTION

User competence has been considered an essential determinant of end-user capability to accomplish tasks in many different fields. In the realm of information systems, user-competence can be defined as the individual's knowledge of the intended technology and ability to use it effectively [1]. Little research has identified or focused upon this concept or its dimensions in the information security field, despite the fact that research repeatedly reports users as the weakest link in security. Measuring the user competence level would contribute to our understanding of the reasons behind user weakness in detecting online security or privacy threats.

Moreover, determining the user competence level has many practical benefits to individuals and more importantly to organisations. For example, organisations often conduct information security training programs without differentiating employees in terms of their knowledge or skills. Such differentiation could make training programs more specialised and meaningful if designed to meet the needs of particular groups of employees. Otherwise, the result is likely to be generic programs with lesser effect [2]. Identifying the dimensions that reflect user competence would simplify the task of classifying users based on their competence and may facilitate the design of tailored training sessions. The research here described investigates the user competence dimensions in relation to detecting online threats in the context of social networks (SN). The main contribution of this study is to propose measurement scales that can be used to model the user competence construct. This is combined with an approach to validating those measurements, with a view to use in future empirical studies.

The rest of this paper is organized as follows. The following section briefly reviews related literature and presents the conceptual basis for the user competence dimensions. Section III describes the approach and technique used to assess the measurement scales and the data collection procedure. The results of the analysis are discussed together with the findings in Section IV. Finally, a summary and our conclusions are presented in Section V.

II. LITERATURE REVIEW

A. User competence

User competence is a critical construct in previous information system research which has been widely examined either as a single-dimension or multi-dimensional construct. However, end-user competence cannot be based upon one type of skill or knowledge. Accordingly, Marcolin and colleagues [3] have investigated various user competence dimensions and their relation to the knowledge domain. Those dimensions can range between *skills-oriented,* which is related to the individual performance in a specific task, *cognitive-oriented*, which is related to knowledge about a specific task, to *affective-oriented*, which is related to the individual's attitude toward the specific task including self-efficacy [4]. Marcolin and colleagues' [3] have concluded that user competence is a multidimensional construct and its dimensions are determined by the research domain.

Existing information system research has widely discussed the importance of examining user competence toward increasing user satisfaction and the usage effectiveness of various technologies [5]. However, little research has investigated its importance in an information security setting. Therefore, based on the user competence conceptualization that has been suggested by previous research [3], the present study proposes examining user competence based on four dimensions which are: self-efficacy (affective-oriented), past experience (cognitive-oriented), privacy and security awareness (skills-oriented). These four dimensions, as shown in Figure 1, can fully conceptualize user competence regarding online risk such as social engineering attacks. For example, if the social network user is aware of the SN privacy issues and the benefits of adjusting privacy settings such as restricting access to their profile, the user would be more competent in avoiding social engineering threats. In the following subsections, the

dimensions of user competence are described in detail with the measurements that would formulate user competence level.

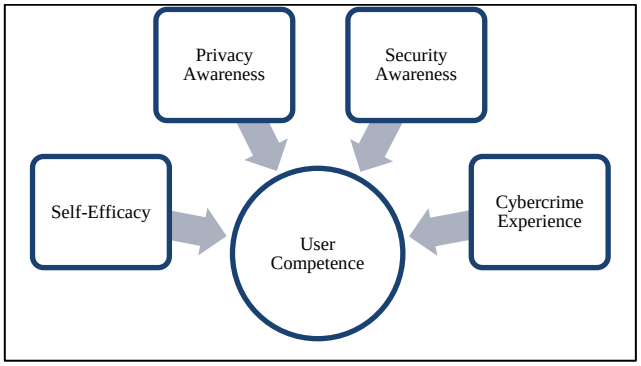

FIGURE 1. Dimensions of the user competence in detecting security threats in OSNs

1) Self-efficacy

Self-efficacy can be defined by the individual's confidence in their ability to protect themselves from SN online threats. Previous research has indicated that self-efficacy can contribute to explaining users' risky behaviour online, as a high level of self-efficacy is more likely to prevent the individual from engaging in risky behaviour online [6]. In our study, the self-efficacy scale is adopted from Milne and colleagues study [6], with some modification to fit the present study context.

2) Privacy awareness

Privacy awareness can be defined as the individual's awareness of actions and behaviour required to protect their personal information in online social networks. Items used to measure the privacy awareness are created based on similar online privacy scale used by Bartsch and Dienlin [7]. The previous study does not include a direct scale that measures user privacy awareness. Rather, it focused mainly on online privacy literacy and investigates the factors that affect it or are affected by it. Online privacy literacy is a general and complex concept that aims to gauge people's knowledge from many dimensions such as laws and legal aspects of data protection, and the technical aspects of online privacy and data protection [8]. The evaluation of peoples' privacy knowledge does not always reflect in their online behaviour. It is important to measure user awareness based on an assessment of online behaviour. Consequently, the items used in the present study aim to measure the individual's awareness of privacy safe practises in social network.

3) Security awareness

Security awareness can be defined as the individual's awareness of actions and behaviour to protect themselves from online social network security threats. The information security literature lacks a validated and accepted measure or technique that can assess individual security awareness in the context of social networks. Organization practitioners always rely on a variety of techniques to measure their users' security awareness, such as counting the number of reported calls to the Helpdesk or measuring the number of accesses to unauthorized websites from their network [9]. However, while such techniques might work for limited and closed environment, they could not measure the users' security awareness for other contexts such as the Internet or social networks. For Internet users, there are other proposed techniques in the literature such as measuring the complexity of the used password [10] or the amount and type of shared sensitive information in SN such as real name, workplace, and address [11]. However, the most common technique used by researchers is gauging the users' security knowledge by their familiarity with the definitions of computer security terms such as phishing, virus, and malware [12].

Notably, there is no specific scale in the literature to measure users' security awareness in the social network context. This makes it important to generate a scale to measure social network-specific information security awareness. The present study has built a scale based on literature recommendations to SN users in order to increase their awareness of the security risks associated with social media usage.

Users' knowledge and behaviour can be reflections of their awareness. If the user practices safe behaviour in SN this can be an indication of high security awareness. Thus, the present study created a scale to measure user awareness based on the amount of user knowledge about security safe practice. Thereby, a high number of security good practices indicates a high level of user security awareness. Security awareness scale items have been taken partially from recommendations and guidelines in information security training programs [13] supported by a scale created to measure secure behaviour in SNs [14].

4) Cybercrime experience

Cybercrime experience can be determined by knowing if the individual has previously faced or fallen victim to any kind of social engineering attacks such as identity theft, phishing, etc. The scale used to measure this factor has been adopted from Rainer and Moore [15]. However, the fourth item in the latter study, which was "Not being able to access online services", has been found to be not significant and removed from the analysis. Therefore, it has also been removed from the present study and replaced by cyber-harassment, which is one of the most common social network attack that has been used and found significant in social network studies [16].

III. METHODOLOGY

A. Content Validity

Content validity can be defined as the extent the measurement used in the test, which can be either questions, tasks, or items, can precisely reflect the constructs that the test aims to measure [17, pp.121]. Content validity is an important issue to be assessed before conducting the original test, in order to guarantee that the selected measurement items fully represent the constructs. Failing to confirm this validity, may lead to serious problems, especially with formative constructs [18].

A review study has found that reliability tests are more commonly adopted in empirical studies, while validity tests have not received much attention from researchers for a long time [19]. However, content validity must be considered when the measurements used in a test are developed or adapted [20]. Even when choosing specific adopted items among others, it is essential to validate whether those selected items adequately represent the sample of other potential items to measure the construct [17, pp.121]. This helps to make sure that the study findings are accurate and may avoid misleading interpretation of the results.

The current study involves measuring a multidimensional construct and most dimension scales used were adopted from previous studies with some adapted and developed scales. Yet, the adopted scales have been developed in different fields than the current study field, which required the addition of some items and change to some of the descriptors in order to fit the present context. This emphasized the importance of conducting a content validation test not only for the adapted scales but also, for the adopted ones.

Several content validation methods have been proposed in the research methods literature such as Anderson and Gerbing's (1991) sorting method [21], Hinkin and Tracey's (1999) rating method that has been illustrated by Yao and colleagues [20], and Schriesheim and Hinkin's item-categorization method [22]. Hinkin and Tracey's (1999) rating method has been recommended [23] as it depends on participant's rating of each item in relation to every construct under study using a Likert scale from 1 (not at all relevant) to 5 (completely relevant). Yet, this method has some limitations. One limitations is the need for a large number of participants if the resulting ratings will be analyzed using one-way between-subjects ANOVA that can only be used if each item-construct rating is done by a different assessor [23]. In addition, the rating method asks participants to rate to what extent every item is related to each construct, which overburdens the participants by increasing the rating attempts [24].

Similarly, the sorting method proposed by Anderson and Gerbing (1991) [21] has some limitations that have been described by Howard and Melloy (2016) [25]. The substantive validity coefficient, C_{sv} index that is used in the sorting method to validate the item is not accurate enough and might lead to wrong conclusions [25]. Moreover, the sorting method forces participants to assign each item to only one relevant construct while the multidimensional nature of our construct makes it difficult sometimes to assign an item to only one dimension (as some items might fit two dimensions with different degrees of relevance).

In our study, we followed Schriesheim and Hinkin's approach [22]. This item-categorization approach has been used widely in the management and communication fields and found to be efficient with multidimensional constructs despite the number of items [26]. Moreover, as the current study focuses on expert assessment, which reflects a small number of assessors, the item-categorization approach is considered suitable as it can provide stable validity with small samples of participants [26].

B. Schriesheim and Hinkin approach

This approach involves sorting and assigning each item to between one and three constructs depending upon the expert's judgment. If the expert thinks the item represents one construct, the expert can assign or tick" √" the intended construct. Otherwise, if the expert thinks the item can indicate more than one construct, the expert will be asked to rank-order the constructs in which the item measures from the highest relevance to the lowest relevance from 1 to 3. After collecting the data, the answers are coded as follows:

- Any tick "√" or "1" answer will be weighted as 3
- Any "2" answer will be weighted as 2
- Any "3" answer will be weighted as 1

Following the recommendations of previous research (e.g. [22], [26]), we only retained items where the percentage of the points assigned by the experts to the intended construct exceeded 60%.

C. Procedure

Participants have been asked to complete a short survey, which consisted of three parts. The first part asking about some demographic factors such as age, gender, and field of expertise. The second part includes the validation matrix. Participants have been asked to judge and align each item in the matrix with its relevant constructs. Items have been listed in the table randomly to control response bias caused by the impact of item order. In the third part, participants have been asked to list the numbers of any statements that they found unclear and to write down any concept or term that they read in the statements that they think needs more clarification.

D. Sample

Schriesheim and colleagues [27] have argued that the appropriate number of samples to conduct content assessment need not be large as the aim of this assessment is to judge theoretically the suitability of the items to measure a particular set of constructs rather than trying to empirically generalize the relationship results. Therefore, according to Schriesheim and colleagues [27], graduate students are considered competent assessors of the content validity tests as their high intellectual ability should make them able to perceive the constructs' definitions and correctly interpret the pool of items. Thus, the selected participants are PhD students in Computer Science from two universities in the UK. Almost 60% of the participants are specialized in the information security field while the rest are specialized in different disciplines, such as cloud computing, digital health, and information sciences. 17 responses have been collected in which 12 of are female and ages range from 25 to 44 years old.

IV. Results and Discussion

Table 1 contains the items for the four constructs and shows the results of content validity for each item. Among the 20 items, there were 4 items (item 7, item 10, item 11, and item 16) with insufficient content validity, as each of these had a percentage of the total points below the 60% threshold.

The self-efficacy and the cybercrime experience items were all scored highly by the participants and no items needed to be changed or removed from their scales. Items 17, 18, and 19 of the cybercrime experience scale have been adopted from an earlier study [15] and their validity is also supported by the result of the current study, as these items received high validity scores of 81.82%, 63.16%, and 81.82% respectively. One new item (item 20) added by the current study to the past experience with cybercrime scale has been given a relatively low score (60.38%).

The privacy awareness items are generally accepted by the participants as they fulfilled the required retention criterion to be included in the scale. In contrast, item 7 failed to exceed the retention cut point as its score was quite low (42.37%). Therefore, this item must be removed from the privacy awareness scale.

Likewise, the consensus among participants regarding item 10, item 11, and item 16 was relatively obvious as their low percentages proved that they could not represent security awareness. Therefore, these three items must be removed from the security awareness scale. It is also worth noting that item 11 (the individual usually reports any malicious accounts to SN provider) was nearly transferred to represent self-efficacy as 45.61% of the total points assigned by participants to this item were in the self-efficacy dimension which was higher than the points assigned to its intended dimension, security awareness, which was only 31.58%. However, this item can't be transferred as it still did not reach the recommended threshold (60%) to be adequate to represent self-efficacy.

TABLE 1. Content Validity Result

	The percentage of the total points			
Items	**SE**	**PA**	**SA**	**EC**
Self-efficacy (SE): The individual's confidence in their ability to protect themselves from SN online threats.				
1. The individual is confident that they can avoid any hazards while using Facebook.	**72.13**	8.20	14.75	0.00
2. The individual is skilled at avoiding dangers while using Facebook.	**64.71**	14.71	14.71	0.00
3. The individual has the knowledge and the ability to secure their Facebook account by adjusting the account settings.	**71.43**	6.35	15.87	3.17
4. The individual has the ability to protect themselves from any online threats while using Facebook.	**66.67**	13.64	9.09	6.06
Privacy Awareness (PA): The individual's awareness of actions and behaviour required to protect their personal information in OSNs.				
5. The individual reviewed the SN privacy policy and they know how to configure it.	20.69	**60.34**	15.52	0.00
6. The individual restricts access to their account by adjusting the privacy setting.	16.67	**73.33**	10.00	0.00
7. On Facebook, the individual does not feel safe regarding their personal data, who can contact them, and the exchange of thoughts and feelings.	0.00	**42.37**	23.73	5.08
8. The individual does not share personal information in SN such as birthdate, phone number, workplace or address.	10.77	**70.77**	10.77	0.00
9. The individual does not share their current or future location in SN, for example, images for their current vacation, or plans for future vacation.	11.11	**62.50**	25.00	0.00
Security Awareness (SA): The individual's awareness of actions and behaviour to protect themselves from OSN security threats.				
10. The individual does not use third party apps (apps that offer new features that are not available in the official version) to access their social networks accounts.	14.04	19.30	**52.63**	0.00
11. The individual usually reports any malicious accounts to SN provider.	**45.61**	12.28	**31.58**	0.00
12. The individual uses password for their SN account different from the passwords they use to access other sites	23.73	0.00	**76.27**	0.00
13. The individual uses a specific new email for their SN account different from their personal or work email.	19.67	0.00	**63.93**	0.00
14. The individual updates their password on a regular basis	16.92	7.69	**75.38**	0.00
15. The individual always reads and pays attention to the security warning messages on Facebook.	6.56	9.84	**72.13**	0.00
16. The individual does not use similar user names for different social media accounts.	9.84	18.03	**52.46**	0.00
Experience with Cybercrime (EC): Has the individual previously faced or fallen victim for any kind of social engineering attacks such as identity theft, phishing...etc.				
17. Has the individual ever experienced somebody stealing their personal data and impersonating them, e.g. shopping under their name, open SN account in their name.	7.27	0.00	10.91	**81.82**
18. Has the individual ever experienced online fraud where goods purchased were not delivered, counterfeit or not as advertised	8.77	0.00	19.30	**63.16**
19. Has the individual ever received emails fraudulently asking for money or personal details (including banking or payment information).	7.27	10.91	0.00	**81.82**
20. Has the individual ever received harassing messages, inappropriate comments, or other persistent behaviours that endanger their safety?	0.00	11.32	0.00	**60.38**

In the qualitative comments, some participants mentioned that they had difficulty to distinguish between the items for security and privacy awareness. Others also mentioned that self-efficacy, security and privacy awareness items can be overlapping as they are very similar to each other. This was clearly seen in the results from Table 1 that for most items, participants have assigned them to those three constructs: self-efficacy, security awareness, and privacy awareness with different relevance. This can remarkably reflect our proposed idea that those items are dimensions that measure the same concept which is user competence.

Regarding the wording of the items, most of the participants found the items to be clear but two participants indicated one item in the privacy awareness which is "I reviewed Facebook privacy policy and I know how to configure it" to be not clear enough. One of them mentioned precisely that the word "configure" is ambiguous here and should be replaced by a more specific word. Therefore, we replaced it with "manage" to remove the ambiguity.

V. CONCLUSION

Cyber-attacks are continuously evolving to catch a huge number of potential victims by using advanced and sophisticated deceiving tactics. Traditional defensive techniques are no longer effective to protect against these enduring threats. Human-related strategies and techniques could provide new preventive solutions in cyber threats research. From this perspective, the proposed measurement test allows determining the competence level of social networks users in detecting cyberattacks and could provide new solutions that rely on monitoring human activities. For example, enriching security alerts by integrating network intelligence and human behaviour. This competence measurement could also help in classifying social networks users into different categories to enhance the benefit of needs-focused training or education sessions.

The objective of the present paper was to detail the validation of the measurement scales for user competence dimensions by using the item-categorization approach, with a view to using those scales and testing them in the future by conducting an empirical study. The result shows that most of the scales' items were significant, with some items being removed due to the controversial opinion of the participants. The result has given evidence that the Schriesheim and Hinkin content validity approach is suitable as a method to validate the constructs measurement in information security research.

One limitation of this study is the relatively small size of the study sample. We should note that most of the experts have been selected precisely based on their knowledge of the field, and this gives reasonable confidence of the credibility of the results. Of course, some of the selected experts are specialized on other disciplines such as cloud computing, digital health, and informatics in order to ensure diversity of opinions.

Our future study will focus more on exploring the relationships nature between the competence dimensions. These relationships can open insights on developing new models that could predict whether or not a particular user is a detector or a potential victim to cyberattacks. Further research can replicate and extend the current results by using different validity methods. Additionally, future research can examine the validity of the user competence dimensions and their measurements in different information system contexts, such as mobile computing, cloud computing, internet-of-things, and e-government. The result from the current study provides a useful starting point for this further work.

REFERENCES

[1] M. C. Munro, S. L. Huff, B. L. Marcolin, and D. R. Compeau, "Understanding and measuring user competence," *Inform. Manag.*, vol. 33, pp. 46–57, 1997.

[2] J. L. Spears and H. Barki, "User Participation in Information Systems Security Risk Management," *MIS Q.*, vol. 34, no. 3, pp. 503–522, 2010.

[3] B. Marcolin, D. Compeau, M. Munro, and S. Huff, "Assessing user competence: Conceptualization and measurement," *Inf. Syst.*, vol. 11, no. 1, pp. 37–60, 2000.

[4] K. Kraiger, J. K. Ford, and E. Salas, "Application of Cognitive, Skill-Based, and Affective Theories of Learning Outcomes to New Methods of Training Evaluation," *J. Appl. Psychol.*, vol. 78, no. 2, pp. 311–328, 1993.

[5] C. Koo and N. Chung, "Examining explorative and exploitative uses of smartphones: a user competence perspective," *Inf. Technol. People*, vol. 28, no. 1, pp. 133–162, 2015.

[6] G. R. Milne, L. I. Labrecque, and C. Cromer, "Toward an understanding of the online consumer's risky behavior and protection practices," *J. Consum. Aff.*, vol. 43, no. 3, pp. 449–473, 2009.

[7] M. Bartsch and T. Dienlin, "Control your Facebook : An analysis of online privacy literacy," *Comput. Human Behav.*, vol. 56, pp. 147–154, 2016.

[8] S. Trepte, D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind, "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)," in *Reforming European Data Protection Law*, vol. 20, Springer Netherlands, 2015, pp. 333–365.

[9] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories," *African J. Bus. Manag.*, vol. 5, no. 26, pp. 10862–10868, 2011.

[10] G. Kiss and A. Szasz, "Level of the Information Security Awareness of the Mechanical Engineering Students," in *Information Technology Based Higher Education and Training (ITHET)*, 2016, pp. 1–6.

[11] N. Abdul Molok, A. Ali, S. Talib, and M. Mahmud, "Information Security awareness through the use of Social Media," in *Information and Communication Technology for The Muslim World (ICT4M)*, 2014, pp. 1–6.

[12] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A Demographic Analysis of Phishing Susceptability and Effectiveness of Interventions," in *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, 2010, pp. 373–382.

[13] E. B. Kim, "Information Security Awareness Status of Business College: Undergraduate Students," *Inf. Secur. J. A Glob. Perspect.*, vol. 22, no. 4, pp. 171–179, 2013.

[14] A. H. Saleh Zolait, R. R. Al-Anizi, S. Ababneh, F. BuAsalli, and N. Butaiba, "User awareness of social media security: The public sector framework," *Int. J. Bus. Inf. Syst.*, vol. 17, no. 3, pp. 261–282, 2014.

[15] B. Rainer and T. Moore, “How Do Consumers React to Cybercrime ?,” in *eCrime Researchers Summit (eCrime)*, 2012, pp. 1–12.

[16] V. Benson, G. Saridakis, and H. Tennakoon, “Purpose of social networking use and victimisation: Are there any differences between university students and those not in HE?,” *Comput. Human Behav.*, vol. 51, pp. 867–872, 2015.

[17] R. J. Gregory, *Psychological testing: History, principles, and applications*, Fifth Edit. 2007.

[18] S. Petter, “specifying formative constructs in information systems research,” vol. 31, no. 4, pp. 623–656, 2007.

[19] A. E. Barry, B. Chaney, A. K. Piazza-Gardner, and E. A. Chavarria, “Validity and Reliability Reporting Practices in the Field of Health Education and Behavior A Review of Seven Journals,” *Heal. Educ. Behav.*, vol. 41, no. 1, pp. 12–18, 2014.

[20] G. Yao, C. H. Wu, and C. T. Yang, “Examining the content validity of the WHOQOL-BREF from respondents’ perspective by quantitative methods,” *Soc. Indic. Res.*, vol. 85, no. 3, pp. 483–498, 2008.

[21] J. C. Anderson and D. W. Gerbing, “Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities,” *J. Appl. Psychol.*, vol. 76, no. 5, pp. 732–740, 1991.

[22] C. a. Schriesheim and T. R. Hinkin, “Influence tactics used by subordinates: A theoretical and empirical analysis and refinement of the Kipnis, Schmidt, and Wilkinson subscales.,” *J. Appl. Psychol.*, vol. 75, no. 3, pp. 246–257, 1990.

[23] S. B. Mackenzie, P. M. Podsakoff, and N. P. Podsakoff, “Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques,” *MIS Q.*, vol. 35, no. 2, pp. 293–334, 2011.

[24] H. Hoehle and V. Venkatesh, “Mobile Application Usability: Conceptualization and Instrument Development,” *MIS Q.*, vol. 39, no. 2, pp. 435–472, 2015.

[25] M. C. Howard and R. C. Melloy, “Evaluating Item-Sort Task Methods: The Presentation of a New Statistical Significance Formula and Methodological Best Practices,” *J. Bus. Psychol.*, vol. 31, no. 1, pp. 173–186, 2016.

[26] J. S. Hornsby, D. F. Kuratko, D. T. Holt, and W. J. Wales, “Assessing a measurement of organizational preparedness for corporate entrepreneurship,” *J. Prod. Innov. Manag.*, vol. 30, no. 5, pp. 937–955, 2013.

[27] C. A. Schriesheim, K. 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 pencil-and-paper survey-type instruments,” *J. Manage.*, vol. 19, no. 2, pp. 385–417, 1993.