CONF-IRM 2013 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2013

The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods

Waldo Rocha Flores
Royal Institute of Technology (KTH), waldorf@ics.kth.se

Egil Antonsen
Royal Institute of Technology (KTH), e.antonsen@gmail.com

Recommended Citation

Flores, Waldo Rocha and Antonsen, Egil, "The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods" (2013). *CONF-IRM 2013 Proceedings*. 44.
http://aisel.aisnet.org/confirm2013/44

The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods

Waldo Rocha Flores
Royal Institute of Technology (KTH)
waldorf@ics.kth.se

Egil Antonsen
Royal Institute of Technology (KTH)
e.antonsen@gmail.com

Abstract

Content validity, the extent to which a measurement reflects the specific intended domain of content, is a basic type of validity for a valid measurement. It has usually been examined using qualitative methods and has not been given as much attention as the other psychometric properties such as internal consistency reliability, indicator reliability and construct validity in the IS field. In this paper, a quantitative approach including the proportion of substantive agreement (P_{SA}), and substantive validity (C_{SV}) was used to examine content validity for 80 items covering eighth domains related to organizational and individual perspectives of information security. The content validity for the organizational perspective was examined using data from a total of 56 content domain experts. Data from 51 experts were further used to examine content validity for the individual perspective of information security. 31 items did not have an adequate content validity, leaving the instrument with 49 items that have been evaluated for their content validity and can be used in future empirically tests of hypotheses in the information security field. To the knowledge of the authors this quantitative method to assess content validity of items in the process of developing instruments hasn't yet been applied in the field information security.

Keywords

Content validity, Information security, quantitative methods, Anderson and Gerbing method.

1. Introduction

The effectiveness and robustness of technical security components has made it more difficult to successfully attack an organization's computer systems using purely technical means. Many attackers have therefore started to attack the humans accessing and using the computers systems by exploiting human insecure behavior and manipulating people into performing actions that benefits the attacker (Applegate, 2009). This development forces organizations' to structure and organize their information security efforts to ensure that risks related to human aspects of information security can be managed effectively throughout the organization. To aid and guide managers in selecting and developing effective ways of organizing information security efforts, appropriate assessment tools are needed. Several instruments have therefore been developed by researchers to support evaluations of information security behavior and understand determinants of such behavior. These instruments have usually focused on investigating individual perceptions of external cues and properties that determine adherence to information security policies and are based on a variety of theories including theory of planned behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010), general deterrence theory (Lee, Lee, & Yoo, 2004) and learning theory (Warkentin, Johnston, & Shropshire, 2011). Other instruments have largely focused on measuring success rates of certain types of security attacks, (Dodgejr, Carver, & Ferguson, 2007), or capturing characteristics that explain an individual's susceptibility to these attacks (Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012). Instruments to measure the effect of key organizational constructs proposed in organizational and individual behavior literature, on information security has, however, not been rigorously examined (Hu, Dinev, Hart, & Cooke, 2012).

This article reports on results towards the development of a measurement instrument capturing organizational and individual perspectives of information security needed to shape information security behavior. In particular, this article reports on the examination of the content validity of a set of items related to these two aspects of information security. Content validity "the degree to which items in an instrument reflect the content universe to which the instrument will be generalized (Straub, Boudreau, & Gefen, 2004, p. 424)", has usually been examined qualitatively (e.g. Brod, Tesler, & Christensen (2009)) and have not be given as much attention as the other psychometric properties such as internal consistency reliability, indicator reliability and construct validity .

Content validation is an assessment that consists of two stages: development and judgment-quantification (Lynn, 2006). The development stage consists of domain identification, item generation, and instrument construction (this stage is presented in section "Conceptual framework"). Judgment-quantification, entails asking a number of experts to evaluate the validity of the items and as a set (DeVellis, 1991). In the present study, the proportion of substantive agreement (P_{SA}), and substantive validity (C_{SV}) is used to examine items for their content validity (the method proposed by Anderson & Gerbing (1991) is introduced in section "Method"). Besides providing a statistical result to assess the adequacy of content validity of each item, the method does not make any implicit assumptions about the direction of the relationship between the items and their corresponding factors or about the correlations between the items themselves. Therefore, it can be used to assess the content validity of either formative or reflective indicators (MacKenzie, Podsakoff, & Podsakoff, 2011). This is a fundamental advantage when developing formative items to capture a construct as a lack of content validity is a particularly serious problem for constructs with formative indicators (Petter, Straub, & Rai, 2007).

The investigated items were tested for their content validity by collecting data using an email survey distributed to content domain experts. The result of the survey is a set of items that have been evaluated for their content validity and can be used for future empirically tests of hypotheses in the information security field. This is the main contribution of the study.

The rest of the article unfolds as follows. In the next section the conceptual foundation for developing the items is presented. Then, the method to assess content validity is discussed together with an outline of the data collection procedure and analysis. In the section that follows the results from the content validity study are presented and discussed. The last section concludes the article.

2. Conceptual framework

The conceptual foundation for developing items representing constructs related to organizational and individual perspectives of information security was established through two studies. These studies follow the recommendations given by MacKenzie, Podsakoff, & Podsakoff (2011) for developing a measurement instrument. Firstly, organizational and individual constructs, that influence information security behavior, were identified using an inductive method approach. In a second study, the nature of the constructs' conceptual domain was specified and content domain experts were surveyed on the relevance and comprehensiveness of the given construct's dimensions. In the following subsections, the identified constructs are presented. For a detailed description of how the constructs were identified the reader is referred to Rocha Flores & Ekstedt (2012) and Rocha Flores & Korman (2012).

2.1 Individual perspective

The identified individual constructs are related to perceptions of organizational information security policies, practices, procedures and the social conditions within an organizational setting. 46 items were generated based on the conceptual definition of each construct. Table 1 depicts the items.

Information Security Leadership (ISL) concerns the information security leader's actions to motivate employees to adopt a security-savvy behavior. The definition of the construct is based on the Transformational leadership concept (Bass & Riggio, 2006). In the context of information security, the concept points out that the leader should articulate a security vision so that all employees can easily and clearly understand what the aim of information security efforts is in the organization. The leader should also show a reasonable level of mastery, and make it clear for each employee what role s/he plays in the organization's information security efforts, what his/her responsibilities are and whom to turn to in case of a concern. The information security leader's actions should portray information security efforts as business-supportively protective and collective and promote understanding and cooperation as a means of achieving and maintaining effective information security. The information security leader's actions should finally set expectations, as well as provide contingent reward (i.e., punishing non-compliance and negligence while rewarding success stories and exemplary behavior).

Information Security Awareness (ISA) concerns an individual's perception of both his/her general knowledge about information security (e.g. value of assets, threat exposure given circumstances, vulnerabilities and risks) and his/her cognizance of the information security policies in an organization in order to shape employee behavior that is conducive to the protection of information assets. The concept is based on the definition made by Bulgurcu et al., (2010) and the findings in Rocha Flores & Ekstedt (2012).

Learning Oriented Environment (LOE) concerns an individual's perception of the support, possibilities and encouragement of learning within the organizational environment. The concept was developed based on Social learning theory (Bandura, 1977; Warkentin, Johnston, & Shropshire, 2011). The concept concerns an individual's perception of the availability of support when performing a work task (e.g., situational support from colleagues or a superior), an individual's perception of verbal feedback being provided regarding information security while performing work tasks etc. (e.g., informal verbal warning, coaching, dialogues or discussions) and observation- and imitation-based learning from colleagues, co-motivated through seeing a colleague successfully perform a task.

Social Information Security Culture (SISC) concerns an individual's perception of shared beliefs and values among colleagues in the work environment (Chow & Chan, 2008). The concept further points out the quality (e.g., richness and friendliness) of social relationships at the workplace.

2.2 Organizational perspective

An individual's perception of information security can be influenced by management actions that promote good information security practices through clear direction, and provide knowledge of what is necessary for managing information security risks (Von Solms & Von Solms, 2006). These actions can be deployed trough security structures, processes and transferring mechanisms. 34 items were generated based on the conceptual definition of each construct related to organizational perspective of information security. Table 2 depicts the items.

Organizational Structure (OS) involve the existence of responsible functions such as senior-level information security executives and the establishment of a committee comprised of business and security personnel (Kayworth & Whitten, 2010). The structure of clear and unambiguous definitions of the roles and responsibilities of the involved parties throughout the whole organization are prerequisites for effective information security.

Strategic Information Security Processes (SISP) refer to a formal and systematic set of activities with the purpose of maintaining an actual picture of assets, threats, weaknesses, existing countermeasures and finally risks, with regards to information security. Further, the concepts refer to the planning for information security (e.g., acquisition of countermeasures, training and education, exercises) and monitoring the state of information security, as well as the performance of information security efforts and countermeasures (e.g., structures, rules or systems) in the organization.

Security Knowledge Transfer (SKT) refers to the process of capturing and sharing knowledge about information security among organizational members through formal and informal information flows. The formal activities aims at training employees on compliance with actual information security policies in the organization and training employees on general information security threats (e.g., threats relevant while browsing the Internet, using e-mail for correspondence, or telephone communication). The informal activities aim at sharing knowledge and experience regarding information security matters (e.g., meetings, seminars or workshops).

Use of IT for Knowledge Transfer (ITKT) refers to the utilization of IT resources (e.g., IT solutions and/or devices) in order to aid spreading, sharing and maintenance of information security awareness and knowledge in the organization.

3. Method

3.1 Rationale for choosing the Anderson and Gerbing method

Methods for quantitatively measuring content validity include experts rating item relevance to the domain of content using a Likert-type rating scale. The proportion of experts who are in agreement about item relevance then provides a quantitative measure of Content Validity Index (CVI), which has become very popular to use in the nursing and health research field. However, the index has been criticized to give different results depending on how it's used (Polit & Beck, 2006).

A promising method to assess the content validity is the method proposed by Hinkin & Tracey (1999) as illustrated by Yao, Wu, & Yang (2007) and recommended by MacKenzie et al., (2011). The raters are asked to rate the extent to which each item (listed in rows) captures each construct (listed at the top of the columns) using a five point Likert-type scale ranging from 1 (not at all) to 5 (completely). However, this method has its limitations. The method includes a one-way repeated measures ANOVA to assess whether an item's mean rating on one construct differs from its ratings on other construct, and because each rater makes multiple ratings for each item, it would only be appropriate to use a one-way between-subjects ANOVA to analyze the data if the ratings of each item on each construct were provided by different raters. This would require substantially more subjects and the test of the item rating differences across the constructs (MacKenzie et al., 2011). Further, it is important to avoid overburdening the raters, and using one-way between-subjects ANOVA would require us to limit the amount of items that we wanted to include in the content validity assessment survey. In a study by Yao, Wu, & Yang (2007) the Anderson and Gerbing sorting method and Hinkin & Tracey method were compared and gave similar results. However, due to the large number of items in our study the Anderson and Gerbing sorting method (Anderson & Gerbing, 1991) was chosen to decrease the time needed to complete the survey and thus avoid overburdening the raters.

3.2 Selection of participants

When selecting people to serve as raters, it is important to make sure that they have sufficient intellectual ability to understand and complete the survey. We therefore argue that the raters both need knowledge in the field of information security and have sufficient intellectual ability. Consequently we approached content domain experts to act as raters.

A thorough selection of experts based on expert criteria is important in order to assure reliability and quality of the study (Weiss & Shanteau, 2003). The experts were identified from scientific articles from searches in professional societies' databases such as the IEEE and in pure indexing databases such as SCOPUS. The search criteria involved combinations of topic-words such as “information security”, “information security behavior” ”information security governance”, and ”information security management” with research area limitations such as ”knowledge sharing” and ”IT governance”. The resulting selections of articles were then manually screened, based on title and abstract (if sufficient) or full content (if necessary) to determine whether the authors should be invited to participate or not. The searches were limited in time to the past three years, i.e. only publications from 2008 and onward were selected. In all, 452 content domain experts were invited to participate.

3.3 The survey

As the experts consulted in this study were geographically widely spread, an e-mail survey was used. Invitations to respond to an electronic survey were sent in October of 2012 to the sample of content domain experts. The survey was hosted by a widely used internet-based application (SurveyMonkey) and open for answering during four weeks. Two reminders were sent to non-responding participants after a first week and a second week in order to increase the response rate (Blaxter, Hughes, & Tight, 2010). The survey consisted of five pages of which the first provided an introduction to the survey, and guidance for completing the survey. The second page included questions used to assess background information of respondents. The two following pages of the survey consisted of two matrixes (one for the organizational perspective containing 34 items and one for the individual perspective containing 46 items) in which definitions of the constructs established in Rocha Flores & Korman (2012) were listed at the top of the columns and the items, that all were randomly ordered, listed in the rows. The experts were asked to read each item and assign it to the construct that they, in their judgment, the item best indicate (Anderson & Gerbing, 1991).

The survey also included questions about the comprehensiveness of the items, i.e. if there are any important items missing to capture the construct domain, and the understandability of the items, i.e. if the items are constructed improperly and if there are any potential misspellings. For each matrix the respondents were asked to give qualitative opinions on the given set of items in order to assure that all items related to the constructs have been taken into account and are constructed properly.

3.4 Analysis

From the responses the two indices proportion of substantive agreement (P_{SA}) and substantive validity coefficient (C_{SV}) as proposed by Anderson and Gerbing where calculated.

The proportion of substantive agreement is calculated in the following way:

$$P_{SA} = \frac{n_c}{N}$$

Where n_c is the number respondents that have assigned the item to the intended construct and N is the total number of respondents. The proportion of substantive agreement can vary between 0.0 and 1.0. A higher number indicate that more respondents have assigned the item to the intended construct.

The substantive validity coefficient is calculated by:

$$C_{SV} = \frac{n_c - n_o}{N}$$

Where n_c and N is still defined as above and where n_o is the most assigned constructs excluding the intended. The substantive validity coefficient can vary between the values -1.0 and 1.0. A positive number indicates that the item is assigned to the intended construct more often than any other construct. Analogously a negative value indicates that the intended construct is assigned more often to another construct then the intended. There are no criterion values for P_{SA} and C_{SV}. In line with the arguments by Yao, Wu, & Yang (2007) on criterion values and due to fact that there are four constructs in both the investigated perspectives of information security we used 0.30 as the threshold value for both P_{SA} and C_{SV}. The expected value for P_{SA}, for instance, is 0.25 if an item is randomly assigned. Thus, choosing 0.30 as the criterion value is higher than 0.25 and items with either a P_{SA} or C_{SV} below 0.30 were deemed to have insufficient content validity.

4. Results and discussions

Out of a total of 452 e-mail requests that where sent 21 bounced or were unregistered from the mailing list. After two reminders 115 had opened the survey and 56 respondents had completed the survey for the organizational perspective (13%) containing and 51 for the individual perspective (11.8%). In the judgment-quantification process, a minimum of three experts are advised by Lynn (2006), while others have recommended from 2 to 20 experts (Gable & Wolf, 1993). In the present study, the number of members necessary for a panel greatly exceeds the recommended threshold.

4.1 Individual perspective

Table 1 contains the items and substantive agreement for each construct for each item and the substantive validity coefficient for the items posited construct. There were 15 items that had insufficient content validity (item 2, 7, 8, 9, 10, 11, 12, 13, 14, 40, 41, 42, 43, 44 and 46) with the cut points for P_{SA} and C_{SV} at 0.30 for both values. Five items were transferred to SISC as they fulfilled the threshold values for transferring items according to Anderson and Gerbing method. One item (item 27) was originally in the ISL construct. Four items (item 36, 37, 38 and 39) was originally in the LEO construct. The results show that all items representing ISA and SISC had an adequate content validity. However, the consensus regarding items representing ISL and LOE is rather low. For instance, item 2 (“The way our top management talks and behaves makes it clear to me what part I play in achieving and maintaining effective information security.”) had a value close to the threshold, but many experts also perceived that the item represent ISA. This result is rather confusing due to the fact that the item explicitly contains the words “management” and “behaves”. Item 9 (“Eventual faults and mistakes with a potential to compromise information security are looked upon as serious in our organization, yet still as a source of learning rather than a reason for punishment”) and item 11 (“Employees in our organization are expected to learn from security weaknesses, faults and incidents (own as well as others') as to promote excellence.”) should not measure ISL, but rather measure LOE. Both items contain the word “learn”, which could have influenced the judgment of the experts. Item 41 (“I feel welcome to ask colleagues for advice or help in case of an information security concern.”) and 46 (“I have had opportunities to observe people at work in order to improve myself with regards to information security.”) were both close to the threshold, but were also perceived by the experts to measure SISC and could therefore not be regarded as items with a sufficient content validity. The same holds for item 42-45.

4.2 Organizational perspective

Table 2 contains the items and substantive agreement for each construct for each item and the substantive validity coefficient for the items posited construct. There were 16 items that had insufficient content validity (item 4, 5, 9, 12, 13, 14, 15, 16, 18, 19, 20, 21, 25, 27, 31 and 33) with the cut points for P_{SA} and C_{SV} at 0.30 for both values. One item (item 7) was originally in the OS construct but the results showed that they fulfilled the threshold values for transferring items to SISP.

The remaining results show that low consensus regarding the content validity of items could be found in all domains. Differentiating between OS and SISP seems to be challenging. For instance, item 5 (“Information security responsibilities are defined for each and every employee.”) was generated to measure OS but there were many experts that believed the item should measure SISP. Further, item 13 (“At some level in the organization, establishment of, changes to and disposal of information security controls is being discussed and decided upon.”) and 15 (“Information security planning is done regularly, in systematic and formalized ways.”) were both generated to measure SISP, but some experts believed that the items should measure OS and therefore they both were deemed to have insufficient content validity.

Item 27 (“Employees with dedicated information security responsibilities are striving to achieve and maintain friendly relationships to other employees.”) were generated to capture the informal security knowledge transfer activities, but the yielded value were far from the threshold. In fact, many experts believed the item should measure OS or SISP. This gives an indication of the challenges that exists when trying to capture concepts that could be interpreted as “vague” and containing “informal” items.
Item 31 (“There is a system, which provides real-time advice on performed tasks, including advice on information security.”) had a value close to the threshold. The item was generated to capture ITKT, but the experts perceived that the items also could measure SISP. One explanation for not having a value over the threshold could be that the item contains a general word “system” and not a specific word such as “IT-system”, which could have confused the panel members.

Domain and item	N	P_{SA}				C_{SV}
		ISL	ISA	SISC	LOE	
Information Security Leadership						
1. Top management in my organization clearly expresses what the aim of the information security efforts is in our organization is.	51	0,69	0,20	0,04	0,08	0,49
2. The way our top management talks and behaves makes it clear to me what part I play in achieving and maintaining effective information security.	51	0,51	0,27	0,10	0,12	0,24
3. The information security leader shows a reasonable level of mastery (knowledge and skills) in the field of information security.	51	0,67	0,22	0,04	0,08	0,45
4. The information security leader portrays information security a collective effort.	51	0,65	0,12	0,18	0,06	0,47
5. The information security leader promotes shared understanding, communication and cooperation as a means of achieving and maintaining effective information security across the organization.	51	0,71	0,08	0,16	0,06	0,55
6. The information security leader portrays information security as a supportively protective effort towards primary business activities and information values, rather than a limiting factor based on formal regulations and best practice.	51	0,63	0,14	0,18	0,06	0,45

7. Employees are required to behave in way as to protect information values and business activities in our organization (also termed due care).	51	0,31	0,27	0,33	0,08	-0,02
8. Employees are required to investigate consequences of their actions given circumstances as to protect information values and business activities in our organization (also termed due diligence).	51	0,27	0,27	0,24	0,22	0,00
9. Eventual faults and mistakes with a potential to compromise information security are looked upon as serious in our organization, yet still as a source of learning rather than a reason for punishment.	51	0,16	0,10	0,27	0,47	-0,31
10. Difficulties to behave in a secure manner towards information assets and business activities are followed up and actively worked with.	51	0,20	0,18	0,41	0,22	-0,22
11. Employees in our organization are expected to learn from security weaknesses, faults and incidents (own as well as others') as to promote excellence.	51	0,08	0,18	0,35	0,39	-0,31
12. Deliberate incompliance or negligence of due care / due diligence is being punished (e.g., through personal feedback with duty reminder, or a formal disciplinary process).	51	0,35	0,18	0,33	0,14	0,18
13. Successful steps to incident-prevention or effective incident handling are rewarded (e.g., through personal feedback and/or benefits).	51	0,18	0,22	0,31	0,29	-0,14
14. Successful steps to incident-prevention or effective incident handling are made visible as to exemplify and encourage such behavior.	51	0,25	0,22	0,35	0,18	-0,10
Information Security Awareness						
15. I am familiar with the content of our organization's information security policy.	51	0,14	0,71	0,08	0,08	0,57
16. I know what the information security policy describes as acceptable use of e-mail.	51	0,08	0,69	0,18	0,06	0,51
17. I know what the information security policy describes as acceptable use of Internet and social media.	51	0,08	0,73	0,10	0,10	0,63
18. I know what the information security policy describes as acceptable use of telephone.	51	0,06	0,71	0,20	0,04	0,51
19. I know what the information security policy requires and forbids regarding management and use of computer passwords.	51	0,04	0,65	0,22	0,10	0,43
20. I know how the information security policy regulates work with and disposal of sensitive information	51	0,08	0,69	0,16	0,08	0,53
21. I know how the information security policy regulates disposal and recirculation of devices.	51	0,10	0,67	0,14	0,10	0,53
22. I know what the information security policy says about installing custom software.	51	0,12	0,73	0,06	0,10	0,61
23. Overall, I am aware of potential information security threats related to my work and the organization's business activities, as well as the negative consequences they may cause.	51	0,06	0,71	0,20	0,04	0,51
24. I have sufficient knowledge about how much it costs my organization to face potential security incidents.	51	0,06	0,69	0,18	0,08	0,51
25. I understand concerns regarding information security and the risks that information security threats pose in general.	51	0,08	0,65	0,22	0,06	0,43
26. In each work situation I am aware of the information security issues that can be caused or allowed for through my actions as well as eventual negligence.	51	0,06	0,65	0,14	0,16	0,49
Social Information Security Culture						
27. In our organization, information security is viewed as a collective responsibility.	51	0,20	0,10	0,65	0,06	0,45

28. I have good relationships with my colleagues and other organizational members.	51	0,16	0,10	0,67	0,08	0,51
29. I am close to my colleagues and other organizational members with regards to communication, cooperation and placement.	51	0,10	0,24	0,55	0,12	0,31
30. Colleagues in my department cooperate well with each other.	51	0,12	0,16	0,61	0,12	0,45
31. Colleagues in my department have a strong feeling of together being one team	51	0,12	0,06	0,69	0,14	0,55
32. In my department, there is a significant perception of having common goals.	51	0,14	0,14	0,59	0,14	0,45
33. Both my colleagues and I agree on the fact that protection of assets such as information, data and our computer environment from getting compromised (e.g., unauthorized disclosed, manipulated, infected by viruses or malware, or suddenly unavailable) is important.	51	0,04	0,18	0,61	0,18	0,43
34. Both my colleagues and I share the same ambitions and vision of protecting information assets from being compromised in our organization.	51	0,14	0,18	0,63	0,06	0,45
35. Both my colleagues and I share and agree on the way collective information security goals are being pursued in our organization.	51	0,06	0,25	0,59	0,10	0,33
36. My colleagues would warn me if they saw me doing something (e.g., using computer, or disposing sensitive information) in an unsecure way.	51	0,06	0,16	0,69	0,10	0,53
37. My colleagues expect me to warn them if I saw them doing something in an unsecure way.	51	0,06	0,20	0,65	0,10	0,45
38. Providing verbal feedback regarding information security between colleagues is generally accepted in my organization.	51	0,06	0,16	0,55	0,24	0,31
39. When I see my colleagues working and behaving in a secure way complying to the information security policies and guidelines, it makes me willing to also do so.	51	0,08	0,16	0,57	0,20	0,37
Learning Oriented Environment						
40. I find that my organization's resources effectively support me to prevent my information assets from eventually getting compromised (e.g., that some sensitive information gets disclosed damaged, or a virus infects my computer).	51	0,16	0,20	0,33	0,31	-0,02
41. I feel welcome to ask colleagues for advice or help in case of an information security concern.	51	0,08	0,12	0,55	0,25	0,29
42. I feel welcome to ask my superior or an information security responsible person for advice or help in case of an information security concern.	51	0,22	0,24	0,27	0,27	-0,29
43. Informal communication or discussions regarding information security phenomena are welcome among colleagues in my organization.	51	0,06	0,14	0,43	0,37	-0,06
44. I feel encouraged to learn or improve at a skill when I see a colleague mastering it.	51	0,04	0,22	0,33	0,41	0,08
45. I have learned to work more secure or improved my information security skills through observing my colleagues at work and taking example.	51	0,04	0,16	0,24	0,57	0,33
46. I have had opportunities to observe people at work in order to improve myself with regards to information security.	51	0,10	0,22	0,22	0,47	0,25

Table 1: Results for the proportion of substantive agreement (P_{SA}) and substantive validity coefficient (C_{SV}) calculations for the individual perspective.

Domain and item	N	P_{SA}				C_{SV}
		OS	SISP	SKT	ITKT	
Organizational Structure						
1. We have an organizational unit with explicit responsibility for organizing and coordinating information security efforts as well as handling incidents.	56	0,70	0,18	0,09	0,04	0,52
2. There is a committee, comprised of representatives from various business units, which coordinates corporate security initiatives	56	0,64	0,16	0,13	0,07	0,48
3. There is a committee, which deals with matters of strategic information security and related decision making.	56	0,59	0,27	0,11	0,04	0,32
4. In our organization, security personnel and line people frequently attend cross-functional meetings.	56	0,27	0,43	0,18	0,13	-0,16
5. Information security responsibilities are defined for each and every employee.	56	0,48	0,27	0,18	0,07	0,21
6. Tactical and operative managers are involved in information security decision making, which is related to their unit, responsibilities and/or subordinates.	51	0,61	0,18	0,20	0,02	0,41
Strategic Information Security Process						
7. In our organization, security responsibles and representatives from various business units meet to discuss important security issues both formally and informally.	56	0,16	0,54	0,16	0,14	0,38
8. Information about risks across business processes is considered.	56	0,21	0,54	0,11	0,14	0,32
9. Information about risk on organizational assets is communicated from top down.	56	0,41	0,29	0,14	0,16	-0,13
10. Vulnerabilities in the information systems and related processes are identified regularly.	56	0,20	0,50	0,20	0,11	0,30
11. Threats that could harm and adversely affect critical operations are identified regularly.	56	0,11	0,61	0,16	0,13	0,45
12. Strategic choices and decisions regarding information security, such as investments, are being discussed and considered in the organization.	56	0,38	0,54	0,07	0,02	0,16
13. At some level in the organization, establishment of, changes to and disposal of information security controls is being discussed and decided upon.	56	0,32	0,57	0,09	0,02	0,25
14. Information security operations, audits and/or exercises are regularly being planned for in the organization.	56	0,18	0,46	0,25	0,11	0,21
15. Information security planning is done regularly, in systematic and formalized ways.	56	0,29	0,57	0,05	0,09	0,29
16. Breaches, damage to information assets and other information security incidents are being reported to a responsible organizational unit, person or a dedicated system.	56	0,39	0,38	0,16	0,07	-0,02
17. Performance of information security controls is measured, for example with regards to the amount of protection they provide as well as the obtrusiveness and performance limitations they pose to personnel, systems and business activities.	56	0,20	0,52	0,16	0,13	0,32
18. In internal interviews or surveys, questions regarding information security are being asked.	56	0,07	0,54	0,25	0,14	0,29
19. Criteria of information security performance are explicit and clear to the responsible personnel.	56	0,45	0,34	0,18	0,04	-0,11
Security Knowledge Transfer						
20. There is an information policy document and/or information security guidelines available to employees.	56	0,29	0,32	0,30	0,09	-0,02
21. Employees receive information about information security policy and guidelines (such as the acceptable use of e-mail, Internet, passwords, telephone, installing additional software etc.).	56	0,09	0,25	0,39	0,27	0,13

22. Formal information security exercises take place in the organization (e.g., training of backup procedures or reaction on security incidents).	56	0,07	0,20	0,70	0,04	0,50
23. In the organization, there is a formal program for information security awareness, training and education.	56	0,11	0,09	0,77	0,04	0,66
24. Employees receive information about information security threats (i.e., which are those, how to avoid falling victim to them and/or how to cope with them otherwise).	56	0,07	0,21	0,54	0,18	0,32
25. There are informal social arrangements, meetings, seminars or workshops directed at sharing experience or knowledge about information security, among other.	56	0,11	0,23	0,46	0,20	0,23
26. The organization provides informal/voluntary consulting and advisory services in information security for its employees.	56	0,11	0,14	0,54	0,21	0,32
27. Employees with dedicated information security responsibilities are striving to achieve and maintain friendly relationships to other employees.	56	0,36	0,36	0,14	0,14	-0,21
28. In the organization, there is an atmosphere where learning is actively encouraged.	56	0,21	0,14	0,57	0,07	0,36
Use of IT for Knowledge Transfer						
29. There is an intranet site dedicated to information security (e.g., general threats and how tos, policy and guidelines).	56	0,11	0,14	0,18	0,57	0,39
30. There is an intranet site, a quality control system or another information system or portal, which contains work- and task-related information security information such as cues, reminders or warnings bound to an action, process or a situation.	56	0,07	0,20	0,14	0,59	0,39
31. There is a system, which provides real-time advice on performed tasks, including advice on information security.	56	0,13	0,23	0,14	0,50	0,27
32. Information technology is actively used to share knowledge and experience regarding information security within the organization.	56	0,05	0,14	0,13	0,68	0,54
33. In our organization, managers are good at using IT to communicate security-related information with employees	56	0,14	0,23	0,16	0,46	0,23
34. The company saves and renews important knowledge on both general information security and threats related to information security onto the computer for easy browsing.	56	0,09	0,16	0,18	0,57	0,39

Table 2: Results for the proportion of substantive agreement (P_{SA}) and substantive validity coefficient (C_{SV}) calculations for the organizational perspective.

4.3 Qualitative comments and item modifications

No comments were received on wording or potential misspellings of each individual item. We explicitly asked for comments to cover this aspect, however, one reason for the lack of comments on this aspect could be that the experts perceived the survey to be time-consuming. Therefore, the experts chose to conduct the item sorting test and leave general comments on the survey and item comprehensiveness, but felt that leaving comments on wording and potential misspellings, for 80 individual items, was far too demanding.

Most of the general comments were encouraging and experts perceived that that the coverage appears comprehensive and well-documented, that the items are relevant and that the approach is interesting. Two general comments pertain to the amount of items and that the survey contains far too many questions. One respondent shared the following.

“The coverage of the survey is comprehensive. Questions could have been simplified a bit as less experienced professionals may have intimidated by the size of question in the matrix (…)

Regarding comments on the understandability of specific items, item 27 is critiqued by one expert for the vague definition of “friendly relationship”.

“Friendly relationship seemed to be a strange question - if there are employees with information security responsibilities, why are not their other tasks discussed.”

Four comments pertain to the conceptualization of the constructs and how they are defined. This is problem that needs more attention as argued by MacKenzie et al., (2011). Two respondents shared the following related to this issue.

“The categories were vague and many of the items could fit in multiple categories. Perhaps some example classifications could be provided to help with understanding what the categories mean and how to discriminate between them.”

“The requested exercise is too informal (the categories proposed are somewhat unclear and the statements to be classified alike).”

Although the constructs were conceptualized in Rocha Flores & Korman (2012) and the items have been categorized accordingly, there are still challenges related to this process. The comments provide further evidence on the challenges regarding informal constructs that can be perceived to be “vague” such as LOE (where only one out of seven items was assessed to have adequate content validity). We therefore highlight the importance of a rigorous conceptualization process that clearly and unambiguously defines the constructs before generating items that are intended to represent the constructs.

5. Conclusions

The purpose of the paper was to examine content validity for 80 items related to organizational and individual information security perspectives. The items were generated based on a conceptual foundation that was established through two previous research studies. The items were tested for their content validity by collecting quantitative data from a sample of 56 respondents (organizational perspective) and 51 for the (individual perspective). 49 out of 80 items were found to have an adequate content validity regarding to proportion of substantive agreement (P_{SA}), and substantive validity (C_{SV}). As the content validity of items has usually been examined qualitatively and have not be given as extensive attention as the other psychometric properties such as internal consistency reliability, indicator reliability and construct validity, the present paper is novel by demonstrating how to quantitatively examine the content validity of generated items in the information security field.

The results shows that the consensus for two domains is high (ISA and SISC). Significant differences of how the experts assess the content validity of items were identified in the remaining investigated domains. We have further provided our opinions on why some items didn’t have an adequate content validity.

The method that was used to assess content validity relies on experts' judgments. However, we would also like to recognize that the finding in the current study may be influenced meanings of items from experts' viewpoints rather than survey respondents' perspective. Future studies could take this into consideration when assessing content validity using quantitative methods.

In the next phase of the research, empirical data will be collected using the key informant methodology in which respondents will be chosen based on their position, experience and professional knowledge. After conducting pilot tests, empirical data will be collected from two key-informants per organization – one respondent from the security organization, and one with a role that includes regular utilization of information technology products and services, e.g. computers, Internet access, electronic mail, etc. (at least ten respondents per organization). To be able to identify differences based on observed heterogeneity, data will be collected from a population with varying characteristics (age, gender, experience etc.) and from organizations covering a comprehensive range of industries in Scandinavia.

References

Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. Journal of Applied Psychology, 76(5), 732–740.

Applegate, S. D. (2009). Social Engineering: Hacking the Wetware! Information Security Journal: A Global Perspective, 18(1), 40–46.

Bandura, A. (1977). Social Learning Theory. Englewood Cliffs, NJ: : Prentice Hall.

Bass, B. M., & Riggio, R. E. (2006). Transformational Leadership (2nd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Blaxter, L., Hughes, C., & Tight, M. (2010). How to Research. McGraw-Hill International.

Brod, M., Tesler, L. E., & Christensen, T. L. (2009). Qualitative research and content validity: developing best practices based on science and experience. Quality of life research□: an international journal of quality of life aspects of treatment, care and rehabilitation, 18(9), 1263–1278.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Management Information Systems Quarterly, 34(3), 523 – 548.

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals in organizational knowledge sharing. Information & Management, 45(7), 458–465.

DeVellis, R. F. (1991). Scale development: Theory and applications. Newbury Park, CA: Sage.

Dodgejr, R., Carver, C., & Ferguson, A. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73–80.

Gable, R. K., & Wolf, J. W. (1993). Instrument development in the affective domain: Measuring attitudes and values in corporate and school settings. Boston: Kluwer Academic.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences, 43(4), 615–660.

Kayworth, T., & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. MIS Quartely Executive, 9(3), 303–315.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707–718.

Lynn, M. R. (2006). Determination and Quantification Of Content Validity. Nursing Research, 35(6), 382–386. Retrieved from http://journals.lww.com/nursingresearchonline/Citation/1986/11000/Determination_and_Quantification_Of_Content.17.aspx

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. MIS Quarterly, 35(2), 293–334.

Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why Do Some People Manage Phishing Emails Better Than Others? Information Management & Computer Security, 20(1), 18–28.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. MIS Quarterly, 31(4), 623–656.

Polit, D. F., & Beck, C. T. (2006). The content validity index: are you sure you know what’s being reported? Critique and recommendations. Research in nursing & health, 29(5), 489–97.

Rocha Flores, W., & Ekstedt, M. (2012). A Model for Investigation Organizational Impact on Information Security Behavior. Seventh Annual Workshop on Information Security and Privacy (WISP) 2012.

Rocha Flores, W., & Korman, M. (2012). Conceptualization of Constructs for Shaping Information Security Behavior: Towards a Measurement Instrument. Seventh Annual Workshop on Information Security and Privacy (WISP) 2012.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. Communications of the Association for Information Systems, 13(1), 380–427.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems, 20(3), 267–284.

Weiss, D. J., & Shanteau, J. (2003). Empirical Assessment of Expertise. Human Factors: The Journal of the Human Factors and Ergonomics Society, 45(1), 104–116.

Von Solms, R., & Von Solms, B. (2006). Information Security Governance: A model based on the Direct–Control Cycle. Computers & Security, 25(6), 408–412.

Yao, G., Wu, C., & Yang, C. (2007). Examining the content validity of the WHOQOL-BREF from respondents’ perspective by quantitative methods. Social Indicators Research, 85(3), 483–498.