https://doi.org/10.48009/2_iis_2009_407-414

EXPLORING THE NATURE OF SECURITY AWARENESS: A PHILOSOPHICAL PERSPECTIVE

Kamphol Wipawayangkool, The University of Texas at Arlington, kamphol.wipawayangkool@mavs.uta.edu

ABSTRACT

Security awareness is acknowledged as one of the true culprits in many failures in information security management, yet very limited amount of literature has explored the nature of security awareness. Although few studies have proposed guidelines of how to study and measure it, the power of those approaches appears to be inherently limited. To fill such gaps, the objectives of this paper are (1) to explore the nature of security awareness based on the theory of learning outcomes, (2) to develop a philosophical conceptualization of security awareness based on the philosophy of scientific realism, and (3) to suggest that multiple methodologies help researchers learn better the nature of security awareness. By resorting to scientific realism, this paper not only provides a richer understanding of the multidimensional nature of security awareness, but points out that researchers should triangulate multiple methodologies to study it. In addition, the application of scientific realism in this paper should alleviate the incorrigible debates around the polarization of positivism and anti-positivism in the field.

Keywords: Security Awareness, Philosophy of Science, Scientific Realism, and Methodology

INTRODUCTION AND LITERATURE BACKGROUND

Both practitioners and researchers have recently emphasized the significance of people's security awareness in information security management (ISM) (e.g. [1, 2, 10, 11, 12, 19, 21, 23]). The 2007 Deloitte Global Security Survey with respondents from 169 major global financial institutions reported that compared to prior years, technical factors did not appear in the list of top priorities, but security awareness and training (48%) was in the top three. It is evident that information security is rather people than technology issues. Regardless of how many technologies are implemented, if people lack their awareness, security breaches are eventually certain to occur. Thus, it can be said that security awareness is a fundamental liability in many failures in ISM. Despite its significance, surprisingly limited number of studies has explored the nature of security awareness (e.g. [15, 20, 21, 23]). Conceivably, such particular scarcity is exponentially due to limited amount of research in information security discipline itself [13]. It is also possible that the true nature of security awareness appears to be quite behavioral, making it perhaps foreign to classical scientific researchers to study [21]. In addition to understanding, to be able to manage people effectively regarding ISM, organizations have to be able to assess people's security awareness. Thus, "what is the nature of security awareness?" and "how to assess or even measure it?" legitimately emerge as two critical questions.

To the best of the author's knowledge, only few studies have responded to both questions either directly or indirectly. The orientation of those studies appears to be either quantitative or qualitative. First, Kruger and Kearney [15] developed a prototype for assessing security awareness in which the model intended to measure knowledge (what a person knows), attitude (how a person feels about the topic), and behavior (what a person actually does). Responding to "what to measure", they further incorporated six key areas (i.e. adhering to policies, keeping passwords secret, using the Internet with care, using mobile devices with care, reporting incidents, and remembering that all actions carry consequences) into each dimension (knowledge, attitude, and behavior). Responding to "how to measure", they developed a thirty-five questions questionnaire that uses a few anchors (true, false, and in some questions, do not know) to measure all the dimensions. Acknowledging their contribution to the field and their mentioned caveats of their prototype, this paper believes that by pointing out limitations, the topic can continue to grow. Firstly, their conceptualization of knowledge, attitude, and behavior appears reasonable, but what exactly is the theory, they mentioned, borrowed from the social psychology? That vague reference unfortunately limits future study to be able to provide stronger justification of or extension to the model. Secondly, while it is absolutely appropriate and reasonable to use a survey to measure all the dimensions (even attitude and behavior), one should not claim that such

few points scale (true, false, and do not know) can appropriately demonstrate reliability and validity of the items, thus inherently limiting the effectiveness of the survey. Incidentally, their study is quantitative-oriented.

The second study pertinent to those two critical questions is Siponen's qualitative-oriented study [20]. The study suggested that qualitative approach is more effective than quantitative approach to motivate people to comply with security guidelines. Pertinent to "what to assess", the study explicitly emphasizes the role of attitude and motivation as though they are the key nature of security awareness. Pertinent to "how to assess", the study provides a list of practical persuasion approaches (e.g. through principles of morals, emotions, rationality, and sanctions) to influence people's attitudes and motivation. Again to point out for future directions, the limitations of the study are as follows. Firstly, their emphasis on attitude and motivation unfortunately spawns an assumption that people actually have all necessary knowledge and only their affective evaluation is significant (i.e., minimizing the importance of knowledge dimension while maximizing that of affective dimension). Second, the absence of systematic framework of how to possibly assess (albeit qualitatively) the level of security awareness after attitudes and motivation are accounted for to some extent limits the usefulness of proposed approach.

The last study found pertinent to those two questions is Thomson and von Solms's qualitative paper [23]. Their study asserts that the goal of security awareness improvement is to change people's ideas and behaviors. Their model places attitude in the middle and posits that attitude interacts with other factors, namely, cognitions, affections, behavior intentions, and actual behavior. It can be deduced that the model responds to the question "what to assess" by proposing that the nature of security awareness in fact comprises all those factors. Then, their study elaborates on how to change a person's behavior basically based on those factors. The methods include changing behavior directly (ignoring attitudes and knowledge), using a change in behavior to influence attitude, and changing attitude through persuasion. To the question "how to assess", they simply mentioned that either direct observation or self-report can be used. Unlike Siponen [20] especially focusing on attitude, Thomson and von Solms [23] pointed out that other significant factors (e.g. knowledge and cognitions) exist and they interact with attitude, a relationship that ultimately affects people's security awareness. Nonetheless, their study provides little information about how to assess or measure security awareness occurring from those factors.

Taken together, these studies suggest that the nature of security awareness comprises multiple dimensions, and that either quantitative or qualitative approach can be used to assess the nature of security awareness. On the other hand, these studies also point out certain limitations future studies can improve and include such as explicit references to theory-in-use for stronger systematic justification of the proposed model, and carefully crafted survey if quantitative measurement is preferred or systematic framework even if qualitative assessment is preferred. However, it is reasonable to conjecture that since security awareness seems to possess multiple dimensions, "why multiple methodologies (i.e. a combination of qualitative and quantitative) cannot be used to assess or even measure those multiple dimensions?" becomes a legitimate question.

To fill in the aforementioned gaps in literature and to tackle the multiple-methods-multiple-dimensions question, the objectives of this paper are (1) to explore systematically the nature of security awareness based on a specific theoretical perspective from relevant literature, (2) to develop a philosophical conceptualization of security awareness based on the philosophy of scientific realism, and (3) to suggest a set of methodologies salient with such paradigm to help better study security awareness. By drawing from the philosophy of scientific realism, this paper not only provides a richer understanding of the nature of security awareness but also points out how to study security awareness in more profound and effective manners. In addition, this paper demonstrates that the principles of scientific realism are particularly appropriate for studying the multidimensional nature of security awareness. The application of scientific realism presented in this paper should also help alleviate the extent of the incorrigible debates around the polarization of positivism and anti-positivism in the field.

THE NATURE OF SECURITY AWARENESS

The overdue question is "then, what is security awareness?" According to the Information Security Forum (ISF) [9], security awareness is defined as the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. Siponen [20] defined security awareness as "a state where users in an organization are aware, ideally committed to, of their security mission". Dhillon [4] elaborated on security awareness such

that "participants should be aware of the need for security of information systems and networks and what they can do to enhance security." This paper refers to the ISF definition because it implies not only the awareness state but also behavioral state, which is arguably the more important state since behaviors should be able to determine whether or how much an individual is actually aware of his or her behaviors and the consequences. Indeed, it is people's misbehaviors that ultimately result in security breaches.

A Theory Foundation

To explore the nature of security awareness, this paper first establishes certain assumptions. First, security awareness is a multidimensional unobservable construct. Second, the level of security awareness can be increased given a combination of appropriate time, education, and experience. Throughout many principles of ISM, security awareness is often associated with security training [1, 2, 10, 11, 12, 19, 21, 23]. For example, since different organizations may have different security policies, organizations should provide security training programs in order to expect that employees will internalize the given information. In short, more learning is expected to be associated with more awareness. Therefore, this paper specifically draws from Kraiger et al. [14]'s *the theory of learning outcomes*, in which the outcomes can be cognitive, affective, and skill-based.

Cognitive outcomes refer to "a class of variables related to the quantity and type of knowledge and the relationships among knowledge elements" (p. 313). Thus, cognitive learning outcomes are not only derived from the static pool of knowledge but also the dynamic processes of knowledge acquisition, organization, and application. In other words, both "know what it is" and "know how to retrieve and use it" are attributed to cognitive learning. *Affective outcomes* refer to "a class of variables encompassing issues such as attitudes, motivation, and goals that are relevant to the objectives of the training program" (p. 319). The logic is that learning also occurs once an individual's values, attitudes, and motivation somehow change (i.e. exposing to new knowledge, an individual's belief system is likely to change and adjust to adopt the new knowledge to some extent). Finally, *skill-based outcomes* refer to "the development of technical or motor skills" characterized by "a goal orientation and a linking of behaviors in a sequentially and hierarchically organized manner" (p. 316). Essentially, an individual develops a skill when he or she can selectively and automatically perform an action with noticeably less error based on an integration of multiple declarative knowledge and discrete steps previously learned.

A Proposed Taxonomy of Security Awareness

Based on the aforementioned assumptions and the theory of learning outcomes, this paper systematically explores the nature of security awareness as follows. Given that security awareness is a multidimensional latent construct, an individual can learn (not necessary exclusively through training programs) to improve his or her level of security awareness cognitively, affectively, and behaviorally. In other words, the taxonomy of security awareness construct incorporates cognitive, affective, and behavioral dimensions.

Specifically to security awareness, *cognitive dimension* refers to 1) the quantity and types of security knowledge including both technical (e.g. the distinctions between viruses, worms, and Trojan horses; the advantages of virtual private networks) and non-technical knowledge (e.g. rules pertinent to organization's security policies), and 2) the relationships among different knowledge (e.g. to comply with a policy entailing secure remote connection to organization's network via a VPN, an individual needs to recall both the information in the policy and how to use a VPN). *Affective dimension* refers to an individual's attitudes and motivation towards security practices and principles both in general and in line with organization's security policies. For example, regarding password setting rules, an individual may or may not perceive its actual usefulness until his or her belief system is changed probably when the underlying reasons are explained, thus leading to an increased level of security awareness. Finally, *behavioral dimension* refers to the development of skills that enables an individual to perform knowingly and automatically both of his or her focal and contextual tasks in a secure manner. In short, when an individual demonstrates a secure behavior knowingly and automatically, the level of security awareness is improved.

In sum, the theoretical nature of security awareness comprises cognitive, affective, and behavioral dimensions. This model is also compatible with the ISF definition of security awareness in that they both acknowledge the significance of not only awareness state (cognitive and affective) but also behavior state (behavioral). Figure 1 illustrates the multidimensional nature of security awareness.

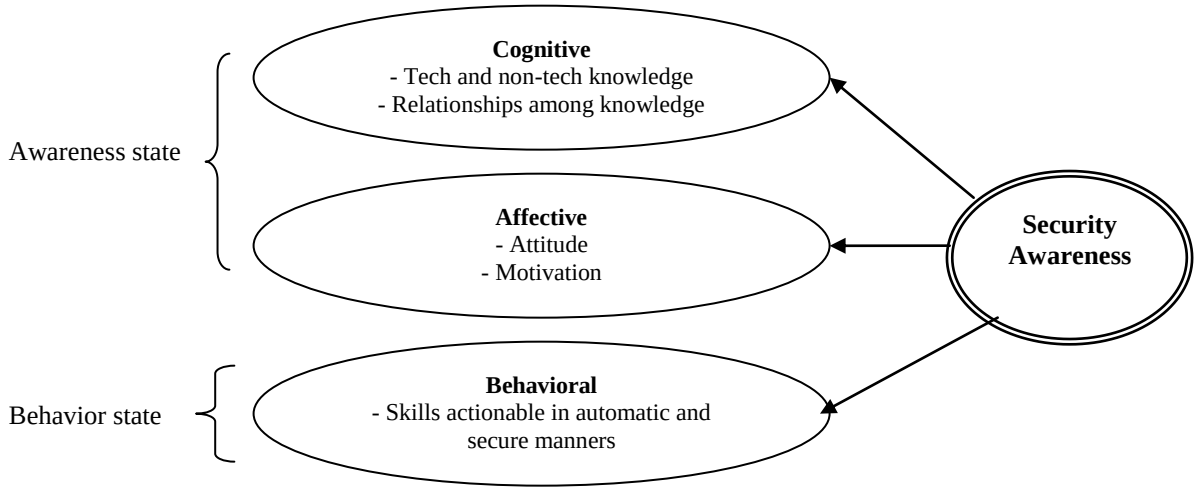

Figure 1. The multidimensional nature of security awareness

A PHILOSOPHICAL CONCEPTUALIZATION OF SECURITY AWARENESS

To provide a more profound understanding of the multidimensional nature of security awareness, this paper attempts to develop a philosophical conceptualization of security awareness based on the philosophy of scientific realism and the proposed taxonomy of security awareness above. This philosophical conceptualization will also lead to a suggestion of multiple methodologies in the next section. To achieve such objectives, this section first provides background of scientific realism to justify the preference of scientific realism as a foundation to investigate the nature of security awareness and then applies the principles of scientific realism to the nature of security awareness. Although the field of philosophy of science has considered that positivism is in fact evolved to logical empiricism [8], some researchers still holds on to the polarization of positivism and anti-positivism (also arguably known as interpretivism). This paper believes that such debate is irredeemable and that it is time for the field to move along with the field of philosophy of science. Indeed, Hunt [6, 8] strongly asserted that scientific realism is a middle ground to reflect the approaches social science researchers have been doing nowadays. Thus, this paper provides a brief background of scientific realism as follows.

Scientific Realism

The philosophy of scientific realism has been spawned from the fundamental limitations of not only positivism and logical empiricism (i.e. believing in knowing with absolute certainty; truth exists) but also relativism (i.e. everything is equally relative; no truth). There exist many versions of realism such as critical realism; nonetheless, scientific realism also covers critical realism [6]. The key tenets of scientific realism are as follows [6]. First, scientific realism proposes that the world exists independently of its being perceived (i.e. there are some abstract things for science to conceptualize about). For positivism and logical empiricism, latent variables do not exist in the world. Second, the function of scientific researchers is to develop knowledge about the world, although such knowledge will never be known with certainty (based on fallibilistic realism). Third, all knowledge claims must be critically evaluated and tested to determine the extent to which they do truly represent or correspond to that world (thus critical realism). Empirical testing is critical, but critical testing is not equal to empirical testing. Critical testing covers all possible methods in both quantitative and qualitative approaches. Essentially, scientific realism posits that in the long run, entities and structures conceptualized in a scientific theory actually exist, and such existence will prove the usefulness and success of science (e.g. vaccines for diseases' entities).

Scientific Realism and Security Awareness

Based on the principles of scientific realism, this paper believes that scientific realism is appropriate for studying the multidimensional nature of security awareness because of the following reasons. First, security awareness is an abstract, unobservable, latent construct, yet it exists for researchers to conceptualize (as this paper does in the previous section). Second, knowledge or findings pertinent to

security awareness may never be absolutely conclusive but accumulative knowledge indeed comprises contribution to the existence of the construct. Similar to the previous section offering a model of security awareness based on prior studies' limitations, this paper contributes to the knowledge of security awareness and the field. Third, based on the theory of learning outcomes and prior studies, it is reasonable to believe that the proposed model is critically and conceptually evaluated. Finally, as literature suggests that better security awareness among people is associated with better security performance of the firm and that without security awareness security vulnerabilities certainly exist, it is deducible that the existence and current body of knowledge of security awareness proves more or less (that is, not with certainty) the usefulness and success of current practices of research.

To develop a philosophical conceptualization of security awareness is for this paper to apply the principles of scientific realism to the dimensions of security awareness as follows. To do so, the classic distinctive albeit intertwined paradigms in information systems (IS) research is briefly discussed at this point. IS research can be classified into either design science or natural science [5, 17]. The goal of design science is to create new and innovative technology-related artifacts. As a result, activities in design science are building artifacts and evaluating their value and applicability. On the other hand, the goal of natural science is to theorize and justify the underlying relationships of those artifacts. As a result, activities in natural science include theorizing and justifying theories of those created artifacts. In short, artifacts from design science give something for natural science to conceptualize about in order to understand more of a phenomenon and to ultimately predict some meaningful relationships (e.g. the interaction between technology and people). It is reasonable to infer that scientific realism can be applied to both the tangibility of design science and the intangibility of natural science as it is applicable to quantum mechanics, biology, and other social sciences such as marketing [6].

Specifically applied to security awareness, this paper posits that scientific realism offers a following conceptualization. First, within *cognitive* dimension, both technical and non-technical knowledge exist. Technical knowledge implies that technology-related artifacts really exist for people to be aware of their characteristics. For example, people have to be aware that security systems (e.g. computer systems) or devices (e.g. biometric devices), which have been theorized and justified, really exist and know how their features can benefit to increase the level of their security awareness. On the contrary, non-technical knowledge implies that concepts or beliefs postulated by people really exist to enable people to apply such concepts to benefit themselves pragmatically in the long run. For example, the beliefs of the benefits of complicated password setting rules are manifested in security policies that help ensure the security of the organization. In other words, scientific realism can associate both the existence of technical knowledge with its tangible (design science-like) nature and the existence of non-technical knowledge with its intangible (natural science-like) nature.

Second, within *affective* dimension, it is clear that the nature of both attitudes and motivation is subjective, non-observable, and intangible (natural science-like). However, based on scientific realism, they really exist because they can be manifested in tangible manners and benefit to their domain. For example, people with positive attitudes and high motivation toward security regulations are likely to cooperate well with those regulations, and such regulations may require certain tangible assets complied with those regulations established; as a result, those people are likely to exert their efforts to seek such complied asset or modify existing one. Again, scientific realism warrants the existence of attitudes and motivation by reasoning that they can result in pragmatic meaningful benefits to the domain.

Finally, within *behavioral* dimension, skills that are actionable in automatic and secure manners are obviously also intangible (natural science is also known as behavioral IS). Similar to affective dimension, scientific realism gives a belief that those skills really exist as they will be manifested in people's secure behaviors to ensure the security principles of the organization. Figure 2 depicts the philosophical existence of security awareness and its dimensions. Nonetheless, as a caveat in scientific realism, it is critical that all knowledge claimed to be useful to the domain is critically tested in order to ensure the true correspondence of its existence to the domain [6]. As mentioned at the beginning that the information security field is still in its early age and evolving, it is premature to claim that the principles of scientific realism have guaranteed the existence and pragmatic benefits of security awareness to the field. In other words, new knowledge, if 'better', can always replace current knowledge. However, as one can see that scientific realism is appropriate for studying security awareness and to move the field forward, it is now reasonable to discuss further how researchers can seek the truth of security awareness under the philosophy of scientific realism.

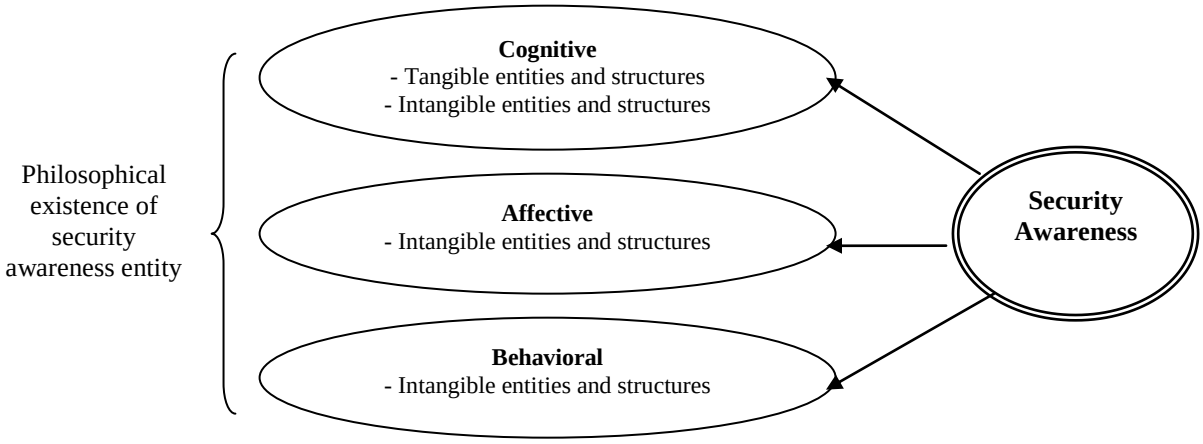

Figure 2. A philosophical conceptualization of security awareness based on scientific realism

METHODOLOGIES FOR SECURITY AWARENESS

Based on the theoretical model of security awareness in the first section) and particularly its philosophical conceptualization in the second section, this section suggests a set of methodologies that can be used to study security awareness. To do so systematically, the implications of the principles of scientific realism are revisited.

To seek the truth or true knowledge, unlike empiricism derivatives (e.g. logical empiricism) which are based on the Humean skepticism, scientific realism is based on the notion of fallibillism [6, 8]. The Humean skepticism asserts that induction logic (i.e. creating theory from observations; bottom-to-top, discovery, exploratory approach) is inappropriate to generate knowledge; as a result, only deduction logic (i.e. testing hypothesized statements, generalizing findings of a set of observations to a theory; top-to-bottom, justification, confirmatory approach) is used in the realm of empiricism. The fallbilism in scientific realism refers to the possibility that both knowledge and its foundation could be false given new evidences. In other words, although knowledge may be never known with certainty, accumulative knowledge in science is still necessary and pragmatically useful. Because of such flexibility, scientific realism embraces a variety of techniques to justify knowledge claims or research findings. As a result, scientific realism considers both induction and deduction equally appropriate to generate knowledge [6]. In addition, those empiricisms strictly rely on empirical techniques, formal logic and rules of probability, while scientific realism is more flexible and especially not strictly to those empirical approaches. Therefore, it is reasonable to suggest that if employed rigorously, all approaches are equally acceptable – whether they are based on deductive or inductive logic, or they are quantitative or qualitative-oriented. Indeed, researchers suggest that triangulation of multiple methods contribute to science [3, 7]. Specifically, an integration of both quantitative methods such as hypothesis testing, survey, mathematical modeling, experimental design and qualitative methods such as case study, action research, ethnography, hermeneutics, and phenomenology, and of exploratory and confirmatory approach contributes to the domain knowledge than a heavy reliance on a single approach [16]. Each method has its own limitation and can be compensated by strengths of other different methods.

For example, to explore users' experience in depth on information security programs, Albrechtsen [1] chose a qualitative approach and found that a user-involving approach is much more effective to influence user awareness and behaviors than formal written document. Therefore, a case study may help study the behavior dimension better than a survey. Indeed, it is doubtful that the similar finding could be found by using a questionnaire. Nonetheless, the limitation lies in the interpretation in which subjective judgment of the researcher can influence to some extent. On the other hand, to be able to measure a number of factors influencing user awareness, using well-designed questionnaire may be more convenient than doing a case study. For example, Choi et al. [2] quantitatively investigated the effects of awareness on organization security performance) based on secondary data. It may be said that a survey is appropriate to measure the level of cognitive dimension of security awareness (i.e. amount and type of knowledge). However, the

limitations include both the issue of reliability and validity of the survey and the data used.

Because of the different nature of each dimension of security awareness, it is reasonable to doubt that one methodology (e.g. using a survey) can capture the true nature of the construct. Therefore, this paper suggests that a triangulation of methodologies is necessary to capture the multidimensional nature of security awareness.

IMPLICATIONS

The implications of this paper are multifold. First, this paper offers the taxonomy of security awareness that is not only theoretically and systematically justified but also compatible with the ISF's definition, implying the significance of both awareness and behavioral state. Second, the philosophical conceptualization demonstrates that scientific realism helps ensure the existence of the dimensions of security awareness and consequently its pragmatic contributions to the field. Third, the principles of scientific realism suggest that to study security awareness in a more effective manner, multiple methodologies are necessary. In other words, since different dimensions appear to possess different nature, one technique is unable to capture their complexity. It is conceivable that one of the reasons that failures in security arena occur due to ineffective assessment and/or measurement of the level of people's security awareness. Incidentally, this reference to scientific realism should also help alleviate the incorrigible debates about the distinction of positivism and anti-positivism in the field.

CONCLUSIONS

Despite its significance, the nature of security awareness has been explored by small number of studies. Limitations in literature appear to be vague conceptualization and less effective of the assessment or measurement methods. To fill such gaps, this paper explores the nature of security awareness specifically based on the theory of learning outcomes, discusses a philosophical conceptualization of security awareness based on the principles of scientific realism, and suggests that multiple methodologies help researchers capture and learn better the multidimensional nature of security awareness. With the application of the philosophy of scientific realism, this paper not only provides a richer understanding of the nature of security awareness but also suggests that researchers should use multiple methods to study it.

REFERENCES

1. Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26, 276-289.
2. Choi, N., Kim, D.J., and Goo, J. (2006). Managerial information security awareness' impact on an organization's information security performance. *Proceedings of the Twelfth Americas Conference on Information Systems*, 2006, 3367-3375.
3. Deshpande, R. (1983). Paradigms lost: On theory and method in research in marketing. *Journal of Marketing*, 47, 101-110.
4. Dhillon, G. (2007). *Principles of information systems security: Text and cases.* John Wiley & Sons, Inc.
5. Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28, 1, 75-105.
6. Hunt, Shelby D. (1990). Truth in marketing theory and research. *Journal of Marketing*, 54 (July), 1-15.
7. Hunt, Shelby D. (1991). Positivism and paradigm dominance in consumer research: Toward critical pluralism and rapprochement. *Journal of Consumer Research*, 18 (June), 32-43.
8. Hunt, Shelby. (2003). *Controversy in marketing theory.* M.E. Sharp.
9. ISF. (2005). The standard of good practice for information security. Version 4.1. Information security forum.
10. Johnson, E.C. (2006). Security awareness: Switch to a better programme. *Network Security*, February, 15-18.
11. Jones, D. (2007). Low cost security tools: Employee awareness. *Security*, November, 90-91.
12. Kelly, C.J. (2006). Awareness Trumps New Security Toys. *Computerworld*, October, 44.
13. Kotulic, A.G. and Clark, J.G. (2004). Why there aren't more information security research studies. *Information & Management*, 41, 597-607.
14. Kraiger, K., Ford, J.K., and Salas, E. (1993). Application of cognitive, skill-Based, and affective theories of learning outcomes to new methods of training evaluation. *Journal of Applied Psychology*, 78, 2, 311-328.
15. Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25, 289-296.
16. Lee, A.S. (1991). Integrating positivist and interpretive approaches to organizational research. *Organizational Science*, 2, 4, 342-365.

17. March, S.T. and Smith, G.F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15, 251-266.
18. Pabrai, U.O.A. (2005). Awareness training: Strengthen your weakest link. *Certification Magazine*, August, 28-29.
19. Schultz, E. (2004). Security training and awareness-fitting a square peg in a round hole. *Computers & Security*, 23, 1-2.
20. Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8, 1, 31-41.
21. Siponen, M.T. (2001). Five dimensions of information security awareness. *Computers and Society*, June, 24-29.
22. Straub, D.W. and Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, December, 441-469.
23. Thomson, M.E. and Von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management and Computer Security*, 6, 4, 167-173.
24. Von Solms, B. (2001). Information Security – A multidimensional discipline. *Computers & Security*, 20, 504-508.
25. Von Solms, B. and Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23, 371-376.
26. Von Solms, R. and Von Solms, B. (2004). From policies to culture. *Computers & Security*, 23, 275-279.