Information & Computer Security

Checking the manipulation checks in information security research

Kent Marett

Checking the manipulation checks in information security research

Kent Marett
Department of Management and Information Systems, Mississippi State University, Mississippi, USA

Received 10 December 2013
Revised 2 March 2014
Accepted 7 March 2014

Abstract

Purpose – An increasing amount of attention is being paid to the human side of information security programs, leading to research designs that require the manipulation of study variables. The purpose of this paper is to highlight a traditional assessment of such designs, the manipulation check, and examine how its absence can undermine otherwise solid research efforts.

Design/methodology/approach – This paper reviews literature from the fields of research methods, organizational behavior and information systems for extant perspectives and viewpoints on manipulation checks, which are then brought into the realm of information security research.

Findings – The possible risks involved with failing to perform manipulation checks are discussed, which include a possibility of making Type II errors. The paper provides further insight on the timing, method and manner in which manipulation checks can be performed.

Originality/value – A disappointing number of research articles in the area of information security fail to report manipulation checks when they should. This paper seeks to remind researchers to perform this vital assessment and to use the results accordingly.

Keywords Information systems, Information security, Methodology, Research methods, Procedures

Paper type General review

Introduction

In keeping with the functional area of information systems (IS) within business organizations, the topic of information security has continually gained more attention from the research community. The number of potential theories, variables, settings and contexts in which information security research can develop and investigate is robust, and it should not be surprising that the number of methods and study designs to help do so is similarly diverse. Many of the traditional study designs used in other areas of IS have been appropriated for conducting empirical research on information security. However, even though these research designs are being used in new research areas, that does not mean that the "old" techniques of testing assumptions and validities no longer apply. One traditional assessment of validity in some empirical designs, the manipulation check, has been observed to be neglected in mainstream IS research (Boudreau *et al.*, 2001), and as this paper shows, that trend continues in research on information security. The importance of conducting manipulation checks cannot be overstated. In empirical studies, tests of assumptions are considered to be critical for interpreting results. It is not sufficient for us, as researchers, to assume that a potential punishment we have designed for violating a company security policy will

Information & Computer Security
Vol. 23 No. 1, 2015
pp. 20-30
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-12-2013-0087

automatically be perceived by subjects as being more severe than another punishment. For the sake of accurately discussing whatever results are attained from the research method, it is essential to measure the subjects' perceptions of the punishment themselves.

To determine whether manipulation checking is common to information security research, a search of the literature was recently undertaken. Twenty-five peer-reviewed articles on information security that utilized experimental and factorial survey designs from the past 10 years were identified. These studies were found in both the premier IS journals and in journals specializing in information security, including articles appearing in *MIS Quarterly* (three articles), *Information Systems Research* (one article), *Journal of Management Information Systems* (four articles), the *Journal of the Association for Information Systems* (one article), *Computers & Security* (three articles) and *Information Management & Computer Security* (three articles), among an assortment of others. Of these 25 articles, only eight reported the use of a manipulation check. That is a rate of 32 per cent, remarkably similar to analyses of IS articles that found manipulation checks were performed 22-30 per cent of the time (Boudreau *et al.*, 2004, 2001). It is not the intent of this paper to single out instances in which manipulation checks should have been conducted but were not. However, it is clear that the use of manipulation checks is not much more consistently used in information security research than it is across the general IS landscape.

Thus, the purpose of this paper is to address the necessity of performing manipulation checks and to discuss the implications of neglecting to do so. In information security research, this issue is increasingly important to verify that artificially manipulated variables perform in the expected manner, as a significant portion of the research utilizes methods that feature manipulations, including field experiments and factorial survey methods. The following section further reviews the purpose of manipulation checks as portrayed by IS research and other referent fields in social science.

Background

Behavioral research often relies on modeling and hypothesizing about abstract concepts, and information security research is no exception. This includes measuring independent variables like *perceived threat severity* and *perceived self-efficacy*, for example, as well as dependent variables like *intention to comply with security policy* or *perceived security effectiveness*. Studying relationships between such variables usually requires a study design that the researchers can control and manipulate, like a randomized experiment, as organizations that will tolerate the disruptions necessary to do so are few and far between (Cook and Campbell, 1979). Thus, researchers develop ways of artificially operationalizing these abstract variables and, in the case of independent variables, frequently use experimental "treatments" to do so. In some instances, the treatment and the independent variables are one and the same, such as when the independent variable involves either the perception of working alone or working in a room with others (Sigall and Mills, 1998). But typically, differences in the independent variable are based on the treatment itself, and subjects who have been randomly assigned to a treatment group are exposed to a different level of the treatment, or "manipulation", than subjects in other groups. Thus, the manipulation impacts the underlying independent variable in such a way as to test its hypothesized relationship with the dependent variable (MacKenzie, 2001). The manipulation check is used to determine if subject perceptions of the independent variable in each group were manipulated in the intended manner and that the experimental treatment was indeed effective.

Manipulation checks are described by Bagozzi (1977, p. 211) as "evidence (independent of the dependent variable) indicating whether the experimental manipulation was indeed effective" providing "stronger evidence for inferring causality". More specifically, manipulation checks can serve at least two purposes. First, the check can affirm that the levels of a treatment were sufficiently different on an inherent property of interest to the study as to merit its use during hypothesis testing, which is a testament to the convergent validity of the treatment. Second, the check can also provide evidence that the manipulation of an independent variable did not have any unexpected impact on other independent variables, establishing a manner of discriminant validity in the study design. This second purpose could be of particular importance in studies in which the treatment seems to otherwise be readily apparent to subjects. For example, Mitchell and Jolley (2010) suggest that, in a hypothetical study manipulating the physical attractiveness of a conversant, a manipulation check could not only help determine that a subject's perceptions of attractiveness were influenced as planned, but that other factors outside the scope of the study, like perceptions of age or wealth of the conversant, were not. This second use of manipulation checks is sometimes referred to as a "confound check".

Straub *et al.* (2007) point out that there are no universally agreed-upon statistical techniques or tests for conducting manipulation checks. Within the IS literature alone, checks have been performed using analysis of variance (Smith *et al.*, 2001), discriminant analysis (Johnston and Warkentin, 2010), Student *t*-tests (Parboteeah *et al.*, 2009) and non-parametric difference assessments like the Mann–Whitney and Friedman tests (Saunders *et al.*, 2011). Moreover, no requisite threshold for determining effective manipulations is established, although tests of significant differences are frequently acknowledged as being valid (Straub *et al.*, 2007). However, manipulations should not be designed with the sole purpose of being statistically significant from each other; they should also be realistic in how they represent the underlying independent variable. This is the "fine line" that Dennis and Valacich (2001) discuss when planning treatments: manipulations should not be too subtle to notice but should also not be so great that the manipulations are hardly comparable to each other. Assessing treatment levels through the use of a manipulation check provides evidence that the levels of a treatment appropriately find the middle ground.

In the following section, common study designs used for empirically studying concepts in information security are reviewed, with the role of manipulation checks highlighted for each.

Research designs using treatments in information security

Experiments and quasi-experiments

Though they may be useful for many common research designs, manipulation checks are most commonly associated with experimental and quasi-experimental methods. They are recommended to be included when describing validation techniques for experiments in both laboratory and field settings, but they are unfortunately reported infrequently (Boudreau *et al.*, 2001). Bagozzi (1977) stated that a common weakness in experiment designs is the tendency to assume away influences like demand cues, evaluation apprehension and other contextual artifacts, but manipulation checks can support claims following data analysis that the manipulated independent variables were indeed significant influences on a dependent variable of interest.

One prominent theory used in information security illustrates the importance of manipulation checking in experimental designs. Protection Motivation Theory (PMT) has provided the theoretical basis for a number of empirical studies in this area, and because it models the cognitive processes undertaken by an individual faced with a potential threat to his or her information security, the variables associated with this theory are self-reported and highly abstract in nature. Experiments are frequently designed with the goal of influencing the PMT cognitive variables in mind, and one commonly used treatment to do so is the exposure of individuals to a fear appeal message. Alternatively, fear appeals may differ in strength between groups. While researchers may suspect one message will induce more fear of the threat in subjects than another, it is incumbent on researchers to empirically confirm those suspicions with a manipulation check of aroused fear (O'Keefe, 2003). Otherwise, the study runs the risk of being exposed to Type I and Type II errors, as is discussed in a later section.

Factorial survey methods

Another common research design used in information security research is the factorial survey method using scenarios (Rossi and Anderson, 1982). In this design, survey respondents are asked to read a vignette involving fictional characters and situations pertaining to the research question. The independent variables appear in the story as manipulated words or phrases within the text. This design is used in information security research particularly when the focus of the study is on socially undesirable behavior which, under normal circumstances, respondents may feel unwilling to admit to committing deviant acts themselves, i.e. social desirability bias. Instead of direct questioning about their own intentions to attempt an unauthorized network intrusion, for instance, the respondent is asked about the story character's intentions. The factorial design allows for treatments to vary from one scenario to another. Thus, manipulation checks are designed to assess that the manipulated wording sufficiently differs between treatment levels so as to determine the influence of the independent variables on psychological states and behavioral intentions (Wason *et al.*, 2003).

An example of a manipulation check in an information security study using scenarios can be found in Chen *et al.* (2012). The wording in the scenarios was designed to manipulate the levels of three variables derived from General Deterrence Theory: perceived punishment, reward and certainty of control over complying with company security policies. The researchers sought to determine that the wording modified between the fictional scenarios influenced perceptions of the three variables, so manipulation checks were conducted through a series of one-item measures. For instance, the check to determine if the manipulated wording for perceived reward was, "If I follow iCorp's security policies, I would be rewarded greatly". The actual text contained within the scenario did not specifically instruct subjects that rewards for compliance would be great, but instead informed them that compliant employees would earn "1 to 5 points added to their merit score" (p. 184); thus, it was up to the subjects to assess whether that was a great reward or not. The researchers later performed one-way ANOVAs to compare the responses between treatment groups and found that the manipulations were not only noticed by subjects but also significantly influenced the underlying variables (punishment, reward and certainty) in the planned manner.

"Cousins" of the manipulation check

Manipulation checks are not the only statistical test for validating treatments. In fact, the term *manipulation check* is occasionally used to refer to one of a number of procedures intended to assess treatments besides those described above. All this naturally adds to the confusion for researchers wishing to understand, and perhaps even replicate, the methods used in a study. This section describes some of the other measures that may pertain to manipulated variables but are not true manipulation checks.

Treatment check

In their review of experimental procedures focusing on independent and mediating variables, Sigall and Mills (1998) noted an unexpected usage of the term *manipulation check*. This involved using the check to determine whether a study participant had noticed the experimental condition that had been manipulated. This type of check, which they later termed a "treatment check", can be useful for filtering out inappropriate data but alone does not demonstrate any comparable differences in the treatment levels of a manipulated independent variable. Sigall and Mills provide the following example as an illustration of a treatment check. Suppose a hypothetical experiment investigates perceptual differences when interacting with employees with different levels of financial expertise. A high-expertise condition might involve communicating with a mutual fund manager, while a low-expertise could involve a video store clerk. A treatment check aiming to determine if a subject noticed the difference in conditions might ask, "Who did you communicate with?" with an incorrect answer producing a valid, systematic way of excluding a subject's data. However, as Sigall and Mills point out, the treatment check does not establish a comparable difference between the two conditions, i.e. evidence of significantly different perceptions of the expertise levels of the two employees. A subject may very well have noticed the manipulation but not perceive a difference in expertise between the two employees. Instead, a manipulation check that empirically measures perceptions of expertise not only provides evidence that a treatment was effective toward manipulating subjects in the intended manner, it also can provide evidence that the treatment was noticed by subjects, essentially serving both purposes.

In their study examining the practices of home Internet users, Anderson and Agarwal (2010) discuss their decision to perform a manipulation check on their independent variables instead of performing a treatment check. They explained that a treatment check that specifically asks subjects if they noticed a manipulation during their experiment would have served to sensitize subjects to identify the independent variables of interest and led them to surmise the goal of the experiment. Their rationale parallels the explanation of Sigall and Mills (1998), in that the manipulation check they designed instead was intended to measure the underlying abstract independent variable influenced by the treatment. Again, it is argued here that the type of check performed by Anderson and Agarwal (2010) fulfills both a treatment check ensuring the manipulation was noticed by subjects and an assessment of the treatment's effects, should a significant difference result.

Involvement and realism checks

Other measures that are sometimes associated with a treatment have also been referred to as "involvement checks". Darley and Lim (1993) and Khan (2011) discuss involvement checks as playing an important role in experiment design, particularly during the pilot test stage. Experiments are vulnerable to the influence of demand cues, which are artifacts within a study's instructions, task or data collection technique that might hint toward the true nature of a study and, thus, potentially bias the results. Involvement checks can be used to determine if a treatment was not only noticeable but also tipped off the goal of the study. Researchers would presumably follow-up with post-experiment interviews with pilot subjects to truly determine if the hypotheses and treatments could be easily ascertained and if any changes to procedures should be made. However, where involvement checks can help assess the unintended effect of demand cues on subject responses, they do not provide evidence of the effectiveness of the manipulations themselves.

It is not uncommon for studies using multiple scenarios to utilize a "realism check" to gauge whether or not respondents can relate to the fictional account described within the vignette. Where manipulation checks pertain more to internal validity of the study design, realism checks are pertinent to the external validity of results (Rossi and Anderson, 1982). Items devoted to assessing the realism of a scenario attempt to ensure that the situation portrayed in the vignette could possibly occur "in the real world", and they may also attempt to determine if the situation is relatable to the subject (Chang, 2006). While it is not required that respondents have personal experience with the situation described in a scenario, a situation should have cues and details that are accessible to the typical respondent, such as those reported in the news media or found in their work lives (Wallander, 2009). While some permutations of a scenario may be eliminated during the design phase due to logical impositions caused by combinations of manipulations (Jasso, 2006), there may be other combinations that are not as readily apparent to researchers, and thus, a realism check should be in order. An example of a realism check in information security research can be found in Siponen and Vance (2010), a study in which one of three separate scenarios were presented to survey respondents. A single-item measure ranging from 0 (not believable) to 100 (totally believable) was administered to assess how each respondent rated the realism of the scenario assigned to him or her. The perceived realism of each scenario can then be compared to confirm one scenario is not significantly less realistic from any of the other scenarios used in the study (Chang, 2006).

Instructional manipulation checks

Finally, in the same spirit of retaining valid subject responses for data analysis as involvement and realism checks, Oppenheimer *et al.* (2009) developed and coined the "instructional manipulation check". Here, the researchers embed a question or an item that does not pertain to the actual study topic, but instead gauges whether the subject has carefully read instructions and examined design materials as hoped or has flippantly completed the questionnaire. Example checks might simply ask subjects to tick the leftmost option on a Likert scale (Cornelissen *et al.* (2011)) or ask subjects to write a word on the questionnaire cover page (Sussman and Alter, 2012). By virtue of a subject incorrectly responding to the instructional manipulation check item, the researcher has grounds to eliminate the entire response set. While no study on information security appears to have conducted anything with the specific name "instructional manipulation check", this technique seems appropriate for both experimental and factorial survey designs. However, this check does not provide any evidence on the suitability of the artificially manipulated variables used in the study.

All the checks described in this section can serve useful purposes for assessing various aspects of experimental and factorial survey designs. However, none of these checks fully substitute for the convergent and discriminant assessments made possible with a manipulation check.

Implications for failing to perform manipulation checks

The purpose of this paper is not merely to explore the need for researchers working within the field of information security to use manipulation checks, but also to discuss the ramifications of failing to do so. This section examines two research designs frequently used in information security research, experimental designs and the factorial survey method using scenarios, using insights on the consequences for failing to ensure manipulation validity held by those who consider them a necessity.

Experimental designs are frequently found in behavioral information security research. Unfortunately, experimenters have often been neglectful in reporting manipulation checks. One hopes that in such cases that the checks were still performed. Straub *et al.* (2007, p. 407) are very clear about their rationale for including checks: "Manipulation validity is mandatory for nearly all types of experimentation. Without these checks, the experimenters cannot be certain which subjects were exposed to the treatments and which were not". This paper argues, of course, that it is not enough to merely ensure that the treatments were noticed by subjects, but that the manipulations adequately influenced subjects in the manner planned by the researchers. Inadequate or "weak" manipulations may fade as quickly as an experiment ends, making their effects difficult to measure (Richins and Bloch, 1986). Weak manipulations also open the experiment up to the likelihood of Type II error (Krueger, 2001; Prentice and Miller, 1992), in which the hypothesized relationship between the independent variable (the treatment) and the dependent variable is wrongly rejected. It must also be stated that weak manipulations may also be the product of the measure used in the check. When an initial check indicates that the manipulation is too subtle, researchers may have the option of using alternate measures for assessing subject perceptions of a treatment instead of drastically retooling the manipulation. In one such example, after a check of a priming manipulation failed to indicate a significant difference between treatment groups, the researchers decided to re-assess a manipulation by conducting a supplemental experiment with a second previously validated measure of the underlying variable (Anderson and Agarwal, 2010). To summarize, experiments featuring weak manipulations are considered highly risky, and as time- and effort-intensive as experimental research can be, information security researchers should make every effort to ensure manipulations are noticeable and effective at the outset.

Another potential problem may reside with the experimental task itself. The task that subjects are asked to complete may be overly demanding in terms of effort or difficulty as to overwhelm whatever manipulations were present (Jarvenpaa *et al.*, 1985). Given that one issue within the field of information security research is the question of computer users avoiding security controls or behaviors that are difficult to perform (Siponen, 2000; Dinev and Hu, 2007), experiments involving subjects interacting with security controls are of relevance. Researchers should be sensitive to the possibility that a task requiring subjects to implement a particular security control may be more difficult than expected. In such a case, whatever effects that would otherwise be produced by the manipulated treatments could be drowned out by the task (unless task difficulty is the independent variable of interest), resulting in Type II error. Jarvenpaa *et al.* (1985) suggest that at least 50 per cent of the subjects should be able to fully complete a task before various types of internal validity, including manipulation validity, are called into question due to subject exertion. In addition to that, manipulation checks showing significant differences between treatment groups can provide additional peace of mind that the task did not overwhelm the manipulation.

For researchers using the factorial survey method, manipulation checks are also highly recommended. The same concern over the effectiveness of manipulated variables that pertains to experimental designs also pertains to factorial surveys. First, manipulation checks can help account for the existence of confounding variables that cannot be included in a scenario or its vignettes. While confounding variables can be problematic in virtually every study design, Wallander (2008) described how the temptation for survey respondents to unconsciously incorporate knowledge about the "real world" to a fictive account described in a vignette is a heightened concern, potentially influencing hypothesized relationships throughout a study. Controlling for the most likely influences can help, but as the number of manipulated conditions per scenario adds up, and the number of vignettes required for respondents to read increases, fatigue likely sets in (Batista-Foguet *et al.*, 1990), increasing respondent susceptibility to confounding variables and other biases as a mental shortcut. Second, Wallander (2008) advocates extreme care when researchers select the levels of multiple manipulated variables contained in a scenario. Should one level be too determinative toward the dependent variable, it could eliminate the possibility of accurately analyzing the effect of the other manipulated variables. Manipulation checks, especially during the pilot phase, could help pinpoint potential problems in this regard and help refine the wording for an extreme level.

It should be noted, however, that there can be entirely valid reasons for not performing a check. Sawyer *et al.* (1995) discuss the cost–benefit analysis of choosing a manipulation check and enumerate potential problems that might occur by doing so. Concerns include the possible restructuring of research designs to incorporate a check, the reluctance of subjects to complete a check when their time is limited and the possibility of the manipulation check to suffer from insufficient trait (construct) validity itself. Sternthal *et al.* (1987) also point out that successful manipulation checks do not guarantee that alternative hypotheses can be ruled out, and instead they suggest planning studies that directly compare rival explanations.

One might also consider the potential for biases resulting from the ordering of manipulation checks. For example, D'Arcy *et al.* (2009) chose not to utilize a manipulation check for fear of sensitizing survey respondents to the treatments conveyed by the scenarios. In such cases, ordering of the check in relation to measuring other variables may mean a great deal. If the manipulation check is measured prior to the measurement of the dependent variable expected to be influenced by the treatment, the check may very well produce the bias D'Arcy and his colleagues hoped to avoid. On the other hand, if the change in the independent variable produced by the manipulation is temporary and not as strong as desired, performing the check after measuring other related variables may not indicate a significant difference between treatment levels where one might have existed before it dissipated (Perdue and Summers, 1986). Ideally, researchers perform manipulation checks during pilot testing to determine whether priming biases or rapidly dissipating effects will be a concern. Other advice to circumvent problems with the ordering of manipulation checks includes the suggestion from Kidd (1976), who recommends the use of holdout samples of subjects for each treatment whose sole purpose would be the assessment of manipulation checks. Others suggest that, though a comparatively uneconomical choice, operationalizing the levels of a treatment in separate studies would eliminate priming problems stemming from the ordering of manipulation checks (Sternthal *et al.*, 1987).

Regardless of whether these or any other issues were first and foremost in the minds of information security researchers when planning studies and deciding how to operationalize independent variables, the fact remains that these or any other issues are not usually stated as being the reason for not reporting manipulation checks, aside from the previous example of the timing bias explanation provided by D'Arcy and colleagues above. Instead, it seems more likely that the concerns and advice supplied by the researchers above were considered too extreme to incorporate, if they were considered at all.

Conclusion

It may seem as if manipulation checks are too basic a research technique as to justify the complete focus of a research paper. However, for a supposedly basic technique, manipulation checks are too often unreported for studies in which their inclusion should be critical. To the contrary, this paper argues that manipulation checks are distinctly important and should be reported front and center in research articles on information security. Furthermore, they are more than basic. To quote Highhouse (2009, p. 557), "good manipulation checks require thought, precision, and creativity". It is hoped that this paper will serve to motivate information security researchers to focus their attention on ensuring their treatments are suitably sound for quality research.

References

Anderson, C. and Agarwal, R. (2010), "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34 No. 3, pp. 613-643.

Bagozzi, R. (1977), "Structural equation models in experimental research", *Journal of Marketing Research*, Vol. 14 No. 2, pp. 209-226.

Batista-Foguet, J., Saris, W. and Tort-Martorell, X. (1990), "Design of experimental studies for measurement and evaluation of the determinants of job satisfaction", *Social Indicators Research*, Vol. 22 No. 1, pp. 49-67.

Boudreau, M.-C., Ariyachandra, T., Gefen, D. and Straub, D. (2004), "Validating is positivist instrumentation: 1997-2001", in Whitman, M.E. and Woszczynski, A.B. (Eds), *The Handbook of Information Systems Research*, Idea Group Publishing, Hershey, PA.

Boudreau, M.-C., Gefen, D. and Straub, D. (2001), "Validation in information systems research: a state-of-the-art assessment", *MIS Quarterly*, Vol. 25 No. 1, pp. 1-16.

Chang, C.-C. (2006), "When service fails: the role of the salesperson and the customer", *Psychology & Marketing*, Vol. 23 No. 3, pp. 203-224.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2012), "Organizations' information security policy compliance: stick or carrot approach?", *Journal of Management Information Systems*, Vol. 29 No. 3, pp. 157-188.

Cook, T.D. and Campbell, D.T. (1979), *Quasi-Experimentation: Design and Analysis Issues for Field Settings*, Rand McNally, Chicago, IL.

Cornelissen, G., Cojuharenco, I. and Karelaia, N. (2011), "One person in the battlefield is not a warrior: self-construal, perceived ability to make a difference, and socially responsible behavior", DEE Working Paper No. 1292, Universitat Pompeu Fabra, Barcelona.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

Darley, W. and Lim, J.-S. (1993), "Assessing demand artifacts in consumer research: an alternative perspective", *Journal of Consumer Research*, Vol. 20 No. 3, pp. 489-495.

Dennis, A. and Valacich, J. (2001), "Conducting research in information systems", *Communications of the AIS*, Vol. 7 article 5.

Dinev, T. and Hu, Q. (2007), "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", *Journal of the Association for Information Systems*, Vol. 8 No. 7.

Highhouse, S. (2009), "Designing experiments that generalize", *Organizational Research Methods*, Vol. 12 No. 3, pp. 554-566.

Jarvenpaa, S., Dickson, G. and Desanctis, G. (1985), "Methodological issues in experimental is research: experiences and recommendations", *MIS Quarterly*, Vol. 9 No. 2, pp. 141-156.

Jasso, G. (2006), "Factorial survey methods for studying beliefs and judgments", *Sociological Methods & Research*, Vol. 34 No. 3, pp. 34-423.

Johnston, A. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Khan, J. (2011), "Validation in marketing experiments revisited", *Journal of Business Research*, Vol. 64 No. 7, pp. 687-692.

Kidd, R. (1976), "Manipulation checks: advantage or disadvantage?", *Representative Research in Social Psychology*, Vol. 7 No. 2, pp. 160-165.

Krueger, J. (2001), "Null hypothesis significance testing", *American Psychologist*, Vol. 56 No. 1, pp. 16-26.

Mackenzie, S. (2001), "Opportunities for improving consumer research through latent variable structural equation modeling", *Journal of Consumer Research*, Vol. 28 No. 1, pp. 159-166.

Mitchell, M. and Jolley, J. (2010), *Research Design Explained*, Wadsworth/Cengage Learning, Belmont, CA.

O'Keefe, D. (2003), "Message properties, mediating states, and manipulation checks: claims, evidence, and data analysis in experimental persuasive message effects research", *Communication Theory*, Vol. 13 No. 3, pp. 251-274.

Oppenheimer, D.M., Meyvis, T. and Davidenko, N. (2009), "Instructional manipulation checks: detecting satisfying to increase statistical power", *Journal of Experimental Social Psychology*, Vol. 45 No. 4, pp. 867-872.

Parboteeah, V., Valacich, J. and Wells, J. (2009), "The influence of website characteristics on a consumer's urge to buy impulsively", *Information Systems Research*, Vol. 20 No. 1, pp. 60-78.

Perdue, B. and Summers, J. (1986), "Checking the success of manipulations in marketing experiments", *Journal of Marketing Research*, Vol. 23 No. 4, pp. 317-326.

Prentice, D. and Miller, D. (1992), "When small effects are impressive", *Psychological Bulletin*, Vol. 112 No. 1, pp. 160-164.

Richins, M. and Bloch, P. (1986), "After the new wears off: the temporal context of product involvement", *Journal of Consumer Research*, Vol. 13 No. 2, pp. 280-285.

Rossi, P.H. and Anderson, A.B. (1982), "The factorial survey approach: an introduction", in Rossi, P.H. and Nock, S.L. (Eds), *Measuring Social Judgments: The Factorial Survey Approach*, Sage Publications, Beverly Hills, CA.

Saunders, C., Rutkowski, A., Van Genuchten, M., Vogel, D. and Orrego, J.M. (2011), "Virtual space and place: theory and test", *MIS Quarterly*, Vol. 35 No. 4, pp. 1079-1098.

Sawyer, A., Lynch, J. and Brinberg, D. (1995), "A Bayesian analysis of the information value of manipulation and confounding checks in theory tests", *Journal of Consumer Research*, Vol. 21 No. 4, pp. 581-595.

Sigall, H. and Mills, J. (1998), "Measures of independent variables and mediators are useful in social psychology experiments: but are they necessary?", *Personality and Social Psychology Review*, Vol. 2 No. 3, pp. 218-226.

Siponen, M. (2000), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 No. 1, pp. 31-41.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Smith, H.J., Keil, M. and Depledge, G. (2001), "Keeping mum as the project goes under: toward an explanatory model", *Journal of Management Information Systems*, Vol. 18 No. 2, pp. 189-227.

Sternthal, B., Tybout, A. and Calder, B. (1987), "Confirmatory versus comparative approaches to judging theory tests", *Journal of Consumer Research*, Vol. 14 No. 1, pp. 114-125.

Straub, D., Boudreau, M.-C. and Gefen, D. (2007), "Validation guidelines for IS positivist research", *Communications of the AIS*, Vol. 13 No. 24, pp. 380-427.

Sussman, A. and Alter, A. (2012), "The exception is the rule: underestimating and overspending on exceptional expenses", *Journal of Consumer Research*, Vol. 39 No. 4, pp. 800-814.

Wallander, L. (2008), "Measuring professional judgements: an application of the factorial survey approach to the field of social work", PhD dissertation, University of Stockholm, Stockholm.

Wallander, L. (2009), "25 years of factorial surveys in sociology: a review", *Social Science Research*, Vol. 38 No. 3, pp. 505-520.

Wason, K., Polonsky, M. and Hyman, M. (2003), "Designing vignette studies in marketing", *Australasian Marketing Journal*, Vol. 10 No. 3, pp. 41-58.

About the author

Kent Marett is an Associate Professor of business information systems at Mississippi State University. He received his PhD in management information systems from Florida State University. His research is primarily focused on online deceptive communication, behavioral information security, the use of technology by work groups and human–computer interaction. His research has been published in several leading journals, including *MIS Quarterly*, the *Journal of Management Information Systems* and the *Journal of the Association for Information Systems*. Kent Marett can be contacted at: kmarett@business.msstate.edu