European Journal of Information Systems (2014) 23, 289–305
© 2014 Operational Research Society Ltd. All rights reserved 0960-085X/14
www.palgrave-journals.com/ejis/

ISSUES AND OPINION

Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations

Mikko Siponen[1,2] and
Anthony Vance[3]

[1]Department of Computer Science and Information Systems, University of Jyväskylä, Finland; [2]Finland Department of Information Processing Science, University of Oulu, Finland; [3]Information Systems Department, Brigham Young University, U.S.A.

**Correspondence: Anthony Vance, Information Systems Department, Marriott School of Management, Brigham Young University, 779 TNRB Brigham Young University, Provo, Utah 84604, U.S.A.
Tel: +1 801 361 2531;
E-mail: anthony@vance.name**

Abstract

The information systems (IS) field continues to debate the relative importance of rigor and relevance in its research. While the pursuit of rigor in research is important, we argue that further effort is needed to improve practical relevance, not only in terms of topics, but also by ensuring contextual relevance. While content validity is often performed rigorously, validated survey instruments may still lack contextual relevance and be out of touch with practice. We argue that IS behavioral research can improve its practical relevance without loss of rigor by carefully addressing a number of contextual issues in instrumentation design. In this opinion article, we outline five guidelines – relating to both rigor and relevance – designed to increase the contextual relevance of field survey research, using case examples from the area of IS security. They are: (1) inform study respondents that a behavior is an ISP violation, (2) measure specific examples of ISP violations, (3) ensure that ISP violations are important ISP problems in practice, (4) ensure the applicability of IS security violations to the organizational context, and (5) consider the appropriate level of specificity and generalizability for instrumentation. We review previous behavioral research on IS security and show that no existing study meets more than three of these five guidelines. By applying these guidelines where applicable, IS scholars can increase the contextual relevance of their instrumentation, yielding results more likely to address important problems in practice.

European Journal of Information Systems (2014) **23**(3), 289–305.
doi:10.1057/ejis.2012.59; published online 12 February 2013

Keywords: information security policy violations; applied science; field surveys; generalizability; content validity; context validity

Introduction

The information systems (IS) field is witness to an ongoing debate on the relative importance of rigor and relevance in research. The rigor side of the debate is typified by the stringent application of research methods, extensive theoretical support, and 'flawless' research designs. The rigor-relevance debate is especially heated within IS behavioral research carried out under the variance model paradigm, in which the aim is to build models that seek to explain or predict, to ever greater degrees, a dependent variable. The IS field's attention to rigor is evidenced by the number of methodological articles, such as those devoted to construct measurement and validation (Straub *et al*, 2004; MacKenzie *et al*, 2011), and measurement of formative constructs (Petter *et al*, 2007; Stafford, 2011), that seek to advance the state of the art.

**Received: 31 May 2010
Revised: 10 May 2011
2nd Revision: 11 January 2012
3rd Revision: 29 February 2012
4th Revision: 3 August 2012
5th Revision: 23 November 2012
Accepted: 4 December 2012**

On the relevance side of this debate, the paramount issue is whether research is of practical relevance. Relevance is especially important in applied fields, such as ISs, in which the aim of research is not only to meet academic criteria, such as providing a theoretical contribution or the application of rigorous research methods, but also to yield highly applicable findings for practice (Benbasat & Zmud, 1999). Whereas basic science 'is performed without thought of practical ends' (Bush, 1945, p. 13), applied science is 'directed toward some individual or group or societal need or use' (Stokes, 1997, p. 8). Thus, relevance is a key criterion of good applied science (Tijssen, 2010).

One way to measure the practical relevance of research is to determine whether IS scholars examine issues relevant to practice in their research. The answer provided to this question by Straub & Ang (2011) is that in this regard IS research is relevant to practice – IS scholars study themes that are important to practitioners. Their argument is that if topics such as IS security are noted as a key concern by practitioners then IS research examining an IS security topic will be relevant. Following Straub & Ang (2011), we call this theme-level relevance. We argue that while such theme-level relevance is important, it does not necessarily follow that research carried out within relevant subject areas are also relevant or valued by practitioners.

While the pursuit of rigor in research is commendable, we argue that further effort is needed to ensure practical relevance. In addition to establishing theme-level relevance, scholars who wish to tackle practical problems (i.e., applied IS research) need to also ensure contextual-level relevance, which goes beyond theme-level relevance. This goal involves whether the specific phenomenon under examination (e.g., the dependent variable) represents an important problem in practice.

While the importance of contextual relevance may appear self-evident, we find that the current discussion and practice of contextual relevance in IS research is unsatisfactory. We argue that while content validity of surveys is often performed rigorously, it nonetheless may lack contextual relevance that is essential. For example, researchers may validate the content of the dependent variable with a review panel consisting of IS professors and students (e.g., using the Q-sorting technique, Moore & Benbasat, 1991). While such a technique may be rigorously applied, it may still lack contextual relevance to practice because academic panel members are likely poor judges of the pressing concerns of practice. In such a scenario, the content of the instrument may be rigorously validated and yet be out of touch with practice.

We argue that IS behavioral research can improve its practical relevance without loss of rigor by carefully addressing a number of contextual issues in survey design. To address this issue, we outline five guidelines to increase the contextual relevance of field survey research (Table 1). In doing so, we offer examples from the practice of information security management, specifically the problem of understanding why employees deliberately violate their organizations' information security policies (ISP), which is a key problem within organizations (PricewaterhouseCoopers, 2010; Puhakainen & Siponen, 2010).

Table 1 Guidelines for field studies on information security policy violations

Guidelines	*Descriptions*
Guideline 1: Inform study respondents that a behavior is an ISP violation	Informing respondents that an ISP violation is involved ensures that participants understand what the violations means in the context of the organization
Guideline 2: Measure specific examples of ISP violations	Measurements of intentions to violate ISPs are more accurate if instrumentation includes contextualized examples of ISP violations, rather than general statements that do not specify the violation type
Guideline 3: Ensure that ISP violations are important ISP problems in practice	Researchers following the applied science paradigm should elicit input from security practitioners to ensure that the ISP violations they wish to study are relevant and important to practice
Guideline 4: Ensure the applicability of IS security violations to the organizational context	Examples of ISP violations should be (1) understood by employees, (2) realistic/applicable for the organizational context, and (3) relevant from the viewpoint of employees' work
Guideline 5: Consider the appropriate level of specificity and generalizability for instrumentation	Scholars should explicitly consider what the appropriate level of contextual specificity is for ISP violations used in their instrumentation, as well as boundary conditions for their theory

To show the importance of these guidelines, we demonstrate from a review of existing ISP violation and computer abuse literature that most studies meet one or two of our guidelines and that no study meets more than three. While our examples are in the context of ISP violations, we believe that these guidelines can aid IS scholars generally to make more informed decisions about how to design field surveys that yield contextually relevant results for practice.

The remainder of this paper is organized as follows: the second section lays out our five guidelines. The third section examines how previous field studies on information security compare against these guidelines. The fourth section offers generalized guidelines for IS scholars as a whole and offers a discussion about their application and limitations. Finally, the conclusion summarizes the key findings of the paper.

Five guidelines for research on employees' deliberate violations of ISPs

In this section, we argue for the importance of five guidelines for researching employees' deliberate ISP violations. However, before presenting our guidelines, we will provide some background into their development as well discuss their basis in applied science. We will also provide a brief overview of ISP and computer abuse research for those unfamiliar with these research streams.

Background

These guidelines are based on the lessons we have learned while researching employees' compliance with ISPs since 1997. Through our research with organizations, we have realized that making employees merely aware of ISPs is not enough (c.f., security awareness research; Karjalainen & Siponen, 2011). Employees need to *comply* with ISPs, and this requires more effort on the part of organizations than simply promoting awareness of ISPs (Siponen, 2000). Further, this realization suggests the need for IS researchers to examine how employees can be encouraged to comply with ISPs.

Pursuing this idea, we have worked with over a dozen large organizations and their chief security officers. This cooperation has involved qualitative interviews of hundreds of employees, and surveys and training sessions of thousands more. The guidelines presented in this section represent the crystallization of lessons we have learned in conducting our research program. These guidelines are not exhaustive, but rather highlight five important, though easy to overlook, research issues regarding employees' deliberate violations of IS security policies.

Description of computer abuse and ISP violation research

We now give a brief overview of computer abuse and ISP violation research for those unfamiliar with these streams of research. Computer abuse has received considerable attention in the area of IS security. This research stream can be traced back to the research of Parker (1976), who first studied and coined the term 'computer abuse'. This term has been consistently defined in the field of ISs as 'the unauthorized and deliberate misuse of assets of the local organizational information system by individuals', including misuse of hardware, software, data, and computer services (Straub, 1990, p. 257; Harrington, 1996; D'Arcy *et al*, 2009).

By comparison, ISP violations are distinguished from general computer abuse in that they are behaviors that violate the ISPs of an organization (Siponen & Vance, 2010). To better illustrate the phenomenon of ISP violations, we refer to the framework of Willison & Warkentin (2013) in Figure 1.

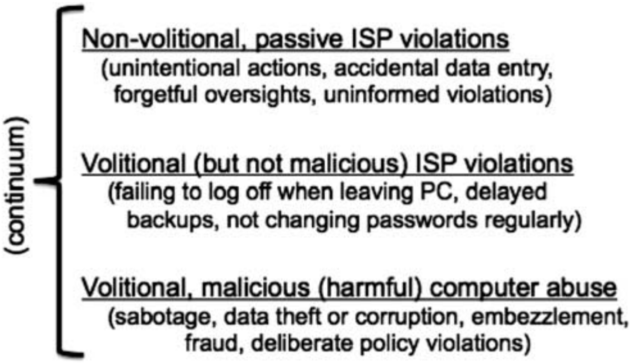
(continuum)
Non-volitional, passive ISP violations
(unintentional actions, accidental data entry, forgetful oversights, uninformed violations)
Volitional (but not malicious) ISP violations
(failing to log off when leaving PC, delayed backups, not changing passwords regularly)
Volitional, malicious (harmful) computer abuse
(sabotage, data theft or corruption, embezzlement, fraud, deliberate policy violations)

Figure 1 Continuum of ISP violations adapted from Willison & Warkentin (2013).

Common examples of ISP violations include using easy-to-guess passwords and not locking one's computer when not at the computer (Siponen & Vance, 2010). Both of these violations could be either non-deliberate or deliberate (Willison & Warkentin, 2013). For non-deliberate violations, employees may violate ISP only because they are unaware of the ISP of their organization. In contrast, in the case of deliberate violations, employees are aware of the ISPs, but choose to violate the ISPs anyway, either maliciously or non-maliciously (Guo *et al*, 2011; Willison & Warkentin, 2013). This latter group is especially challenging to address, because promoting greater awareness of ISPs has little effect on their behavior (Siponen, 2000; Stanton *et al*, 2005).

In terms of method, field surveys are by far the most prevalent method for examining ISP violations. This is because ISP violations are conducted by organizational members, and field surveys provide an effective and rigors means of studying organizational phenomena (McGrath, 1981). In addition, researchers have increasingly employed scenario-based field surveys (e.g., D'Arcy *et al*, 2009; Siponen & Vance, 2010; Hu *et al*, 2011). This method uses written scenarios that 'present subjects with written descriptions of realistic situations and then request responses on a number of rating scales that measure the dependent variables of interest' (Trevino, 1992, pp. 127–128).

Finally, we hasten to point out that our guidelines are designed to apply only to field surveys using variance models, in which independent variables are used to statistically explain or predict dependent variables, which in our case employees violations of ISPs (Burton-Jones *et al*, 2012). This does not mean that the variance model approach is superior to process models or qualitative research, only that our guidelines are not tailored to these approaches.

Guideline 1: inform study respondents that a behavior is an ISP violation

In order for scholars to study deliberate violations of ISPs, respondents must be aware that the actions in question are violations of an ISPs. At issue is content validity, a key consideration in the development of instrumentation (Boudreau *et al*, 2001). As Straub *et al* (2004, p. 384) note:

> Content validity is an issue of representation. The essential question posed by this validity is: Does the instrumentation (e.g., questionnaire items) pull in a representative manner from all of the ways that could be used to measure the content of a given construct?

Applied to our context, when a *deliberate violation of an ISP* is the phenomenon of interest, failing to specify in the instrumentation that an action violates IS policy diminishes content validity. This is because the instrumentation does not adequately represent the construct of deliberate ISP violations. As a result, measurement error occurs, subsequent tests of internal and statistical conclusion validity may be compromised, and 'all other scientific conclusions are thrown into doubt' (Straub *et al*, 2004, p. 383).

The issue that this guideline addresses is perhaps best illustrated with an example. We will use the measurement of ISP violations using scenarios, as is common for studies of computer abuse and violations of organizational norms (O'Fallon & Butterfield, 2005; Siponen & Vance, 2010). However, please note that Guideline 1 applies equally well to traditional survey items, not just scenarios. After reading each scenario, the respondent typically answers using a Likert-type scale to indicate his or her inclination to behave in the same way as the character in the scenario.

> Scenario 1A: Matt is working on a software development project. He emails confidential information to the client without encryption.
>
> Scenario 1B: Matt is working on a software development project. He knows that his company has an explicit ISP that requires that all information labeled 'confidential' be encrypted if emailed to clients. Matt emails confidential information to the client without encryption.
>
> Scenario 2A: Matt finds a USB drive lying on a table in the office lobby and is curious to see to whom it belongs. He takes it back to his desk and inserts the drive into the USB port of his computer.
>
> Scenario 2B: Matt finds a USB drive lying on a table in the office lobby and is curious to see to whom it belongs. Matt knows that accessing USB devices from unknown sources is a violation of his organization's ISP. However, he takes it back to his desk and inserts the drive into the USB port of his computer.

The problem with Scenarios 1A and 2A is that they do not state whether the action described is a violation of an ISP. If the scenarios do not state that an action is a violation of an ISP then we do not know whether the respondents recognized the described behavior as a violation. Thus, we cannot determine whether they would intentionally choose to violate the policy.

Guideline 1 is especially important given that employees are often not aware of their organization's ISPs (Karjalainen & Siponen, 2011). There are several explanations for this. First, policies differ from one organization to another, and privacy laws vary from country to country. We use the issue of non-work-related web browsing (or cyberloafing) as an example. With this issue, there are organizational and even departmental differences as to whether the use of the Internet for non-work-related purposes is categorized as an ISP violation. In addition, there are even contextual differences within an organization. For example, in one organization in which we studied ISP violations, the use of online bank services for employees' personal use was accepted, while the use of other non-work-related web services was not. Another problematic situation for employees is the case in which ISP violations are common at the organization and colleagues may encourage actions in violation of an ISP. An example of such a case is sharing passwords for a hospital's patient record system. While such an act is a violation of the law in Finland, in our experience doctors may view such password sharing as an effective practice that saves time.

Second, respondents may not have been personally impacted by security breaches and may not have learned the importance of good information security principles (Karjalainen & Siponen, 2011). As a result, employees may not intuitively understand why some behaviors could pose a threat to an organization's security and may not intuitively know that certain actions are ISP violations. This is another reason why the violation should be stated in the survey instrument.

Third, respondents may be ignorant of the specific points of ISPs. When general statements are used in the instrumentation, we are not able to discern whether employees are really aware that certain behaviors are security policy violations. Consider a traffic rule analogy. One may say that he or she complies with traffic rules, but if we ask him or her a specific question, such as, 'Do 5-year-olds need to use a child seat in a car?' the respondent may not know the answer. On the basis of our experience with surveying and interviewing employees in organizations, we argue that the same applies to ISPs.

For example, as part of a past research project at several organizations, we surveyed employees and found a high rate of compliance in response to generic measures, such as 'I comply with information security policies'. However, these results were in conflict with the perception of security staff of the organizations who sponsored our research; from their observations, they believed that employee compliance with ISPs was low. To investigate their suspicions, we subsequently surveyed employees with multiple-choice questions about the content of the organization's ISPs. The results showed that employees overwhelmingly failed to answer the multiple-choice questions correctly, implying poor recall of the actual content of the ISPs. We obtained this result even though these same individuals reported high levels of compliance with policies when surveyed regarding generic measures.

We have found similar results in qualitative interviews of over a hundred employees belonging to different organizations. If employees do not know what the ISP says, how can they reliably report that they are compliant with it? By explicitly stating in the measurement of the dependent variable that an ISP violation is involved, researchers eliminate the possibility that respondents fail to recognize ISP violations.

Some researchers may be reluctant to identify a behavior as an ISP violation because of the risk of social desirability bias. Given the sensitive nature of ISP violations, it is entirely possible that respondents' desire to appear compliant will bias the results. However, previous research reports that guaranteeing the anonymity of survey results helps to reduce the likelihood of social desirability bias (Robinson & Bennett, 1995). Our experience supports this. Another solution is to randomly administer two versions of the same instrument: one stating explicitly that the dependent variable describes an ISP violation, and the other not. In subsequent analysis, a *T*-test may be used to detect whether the respondents answered the dependent variable differently depending on whether they were told that an ISP violation was involved.

Guideline 2: measure specific examples of ISP violations

Measurement items fall on an abstraction continuum between the abstract and general and the concrete and detailed. Items that are more abstract are more easily generalizable across populations, but as a consequence tend to be less precise (Hui & Triandis, 1985). In this section, we argue that studies of deliberate ISP violations should measure concrete types of ISP violations. This means that researchers should avoid general statements, such as 'I comply with information security policies' (actual behavior as the dependent variable) or 'I intend to comply with information security policies' (intention as the dependent variable), in their surveys. Rather, we argue that IS scholars should specify the violation in the measurement of the dependent variable, when using either scenarios or traditional survey items. There are at least three reasons for this.

First, general statements assume that there is no difference between different types of violations. In fact, differences in people's willingness to knowingly violate different types of ISPs may exist. These may be impossible to tease out using general instrumentation statements, such as 'I intend to comply with ISPs'. Bulgurcu *et al* (2010, p. 21) specifically state this issue as a limitation of their study, saying that their instrument 'captures compliance at a high level of abstraction', and recommend that future research use detailed examples of violations to 'reveal the differences in an employee's intentions to comply with specific rules and regulations'.

Criminologists have long pointed to the importance of context in understanding norm-breaking behavior (Klepper & Nagin, 1989) since 'the situational context of decision making and the information being handled will vary greatly among offenses' (Clarke & Felson, 1993, p. 6). Furthermore, the result of 'posing vague questions' is that 'each respondent will answer in terms of his own mental picture of the task before him' (Alexander & Becker, 1978, p. 93), essentially forcing respondents to impute circumstances in which they would consider committing an offense (Klepper & Nagin, 1989; Bachman *et al*, 1992). The solution to this problem is to present respondents with instrumentation that is 'as concrete and detailed as possible' (Alexander & Becker, 1978, p. 93). While ISP violations may not be crimes, the aforementioned studies are applicable because criminology explains 'any deviant behavior that violates social norms, whether or not such behavior also violates the law' (Akers & Sellers, 2004, p. 2).

Second, respondents may report that they are compliant with ISPs generally, but they may still violate specific policies. Again, using a traffic analogy, if a person were asked whether he or she complies with traffic laws, the answer might be yes. However, if this same person were asked whether he or she would drive five miles over the speed limit or occasionally jaywalk, the same person might give a different answer.

Criminologists term this phenomenon the 'metaphor of the ledger' (Klockars, 1974), which means people believe that their general compliance with laws or norms outweighs or compensates for particular violations (Piquero *et al*, 2005). Thus, a person who adheres to laws generally may claim to be law-abiding, even though he or she may regularly violate specific laws. We have observed in our own research that employees tend to report that they comply with the ISP in general, yet they may regularly violate various specific ISPs. In our interviews asking about compliance through generic questions such as 'Do you comply with information security policies?' the rate of compliance was high, yet employees reported differently when they were asked whether they complied with specific ISPs.

Third, collecting data about specific types of violations provides researchers and practitioners with actionable insights into specific violations. On the other hand, because generic questions do not refer to any specific act, respondents need to use their memory and imagination to determine what 'policy' is. This raises the possibility that neither IS scholars nor respondents know which security behaviors are in question. From the perspective of applied research, such responses are of little practical value, because how can researchers effectively change specific behaviors if they do not know the *status quo*?

In summary, when studying deliberate ISP violations, we suggest using specific types of violations in the survey instrumentation. Doing so will provide more accurate measures of those willing to deliberately violate ISPs. However, while we advocate the use of specific measures, we do not want to rule out the use of generic measures. Instead, we urge scholars to recognize the potential limitations of generic measures and to carefully justify their use when appropriate.

Guideline 3: ensure that ISP violations are important ISP problems in practice

Applied science suggests that studied phenomenon should be of practical relevance (Niiniluoto, 1993). In accordance with this perspective, our third guideline suggests that studies of deliberate ISP violations should ensure that the types of violations examined address a truly relevant issue in practice. While we suggest examples below regarding how the practical relevance of the dependent variable can be determined, the more important point is that authors should make such considerations explicit and report whether the dependent variable actually represents an important ISP violation.

A good way to determine highly relevant ISP violations is to identify those violations that are both common and of high potential impact. A violation may be common, but not important from the perspective of IS security. For example, visiting a well-known online news site may be common, but it may not have IS security consequences. Similarly, cyberloafing, or non-work-related web use, could be a common computer abuse issue (Aftab, 2003). However, cyberloafing is typically not an IS security issue. On the other hand, some IS security-relevant problems may be catastrophic in their consequences, but highly unlikely to actually occur, for example, an employee bombing a company data center.

Given these points, how can the importance and relevance of ISP violations be established and ensured? First, when performing field surveys within an organization, the most relevant and important violations are often – thought not always – described in the organization's ISPs. Second, it is useful to interview those who are involved in the creation and maintenance organizational ISPs. Obviously, undergraduate students and home users typically do not design ISPs. On the other hand, security professionals often are. If ISP violations are the phenomenon of interest, it makes sense to interview people responsible for designing, maintaining, and enforcing ISPs.

Drawing an analogy to software development, if scholars wish to examine the key problems in software development, it is reasonable to start by interviewing software developers who experience these issues, rather than people who do not actively develop software and whose familiarity with software development issues is therefore less current.

In our experience, the person who has the most experience in designing or maintaining security policies is often the information security manager, or chief information security officer, of the organization. In our research, we have observed that information security managers often have a better understanding of what violations are relevant and important to the organization, *vis-à-vis* specialized network engineers who may be experts in network security, but lack a holistic picture of ISP violation issues.

Alternately, the person most knowledgeable of an organization's ISPs could also be an outside consultant or a security expert within the organization. The title is not important, but the person's familiarity and experience with ISPs is. If such a person cannot be identified or does not exist, we suggest polling that information security across multiple organizations to identify ISP violations that are both commonplace and important.

In contrast, non-security-related employees of the organization may know whether an ISP violation is common (which alone is important information), but we argue that they have difficulty recognizing whether violations are also an important problem to the organization. This is one reason why employees have a hard time complying with the ISPs (Puhakainen & Siponen, 2010). However, employees do have experience that can help them validate contextual issues relating to ISPs (please refer to Guideline 4 below).

To elicit feedback from security practitioners, we suggest three approaches. First, scholars may develop a list of violations based on a literature review, and then let practitioners rank the relevance of these violations. Second, for scenario-based surveys, multiple scenarios could be developed, which information security managers could then rank and comment on. A third method is to use an inductive approach, starting from a clean slate and asking practitioners to name their most concerning ISP violations. The belief elicitation process (Limayem & Hirt, 2003), content analysis, and grounded theory are examples of such an approach.

Finally, we do not wish to suggest that security managers or practitioners dictate which topics scholars study. Obtaining input from practitioners is simply a practical way of determining practice relevance. However, we observe that sometimes important security problems loom on the horizon that are not initially recognized by security professionals. In such cases, it is perfectly reasonable for researchers to study the phenomenon based on other indicators of practical relevance, such as theory or empirical findings. In any case, applied research studies should discuss how practical relevance of ISP violations examined was established.

Guideline 4: ensure the applicability of IS security violations to the organizational context

A form of validity closely related to content validity is context validity, which 'is concerned with the social dimensions of a task, including the setting of the task' (Weir, 2005, p. 284). If the context of an instrument is not applicable or recognizable to respondents, measurement error will likely result. Because ISP violations are an organizational phenomenon, it is critical that survey instrumentation be contextualized for employees of the target organization. This means that the instrument needs to be (1) understood by employees, (2) realistic/applicable for the organizational context, and (3) relevant from the viewpoint of their work. Thus, Guideline 4 should go hand-in-hand with Guideline 3. This fourth guideline applies to both dependent and independent variables.

An important consideration is the possibility that the terms and language of the formal ISP differ from those in actual use. For example, a formal ISP may use a technical term, but in practice employees may use a different word.

Table 2 Examples of different levels of specificity

Types	*Examples from measurement items*	*Behavioral generalizability assumptions*	*Examples from literature*	*Explanations*
Context-free specification of violations	'I use easy-to-guess passwords'	Assumes generalizability in terms of behavior across different contexts and systems	'I intend to use anti-spyware software' (Johnston & Warkentin, 2010a)	Specifies the violation type, but does not specify the context
Specific to context	'I use easy-to-guess passwords for work systems'	Assumes that context is the boundary condition	'[Hannu's company] has a strict policy that each computer workstation must be password-protected and that passwords are not to be shared' (Siponen & Vance, 2010)	Specifies the violation type and the context or other boundaries Does not specify the type of systems
Specific to type of system	'I use easy-to-guess passwords for human resource systems'	Assumes that type of system is the boundary condition	'[Seija's] department uses an inventory procurement software application program to make inventory purchases. To ensure that only authorized individuals make inventory purchases, the company has a firm policy ...' (Siponen & Vance, 2010)	Specifies the violation type and the context or other boundaries Specifies the type of system
Specific to a particular system	'I use an easy-to-guess password for the SAP system'	Assumes that the particular system is the boundary condition	Currently, there is no example in the literature	Specifies the violation type and the context or other boundaries Specifies a particular software product or system

Similarly, an ISP policy may state a certain high-level requirement, for example, that remote network access be performed via an encrypted connection, but not name specific software to meet the requirement. In such a scenario, employees may use the name of the software used to implement the ISP on a daily basis, yet without interviews or observation it would not be clear whether or not employees were compliant with the policy.

Another potential issue is the name of ISP documents. Organizations may have multiple information security documents, each with a different scope and name, for example, 'security policy' compared with 'security procedure'. When asking respondents about ISP compliance, it is important to use the correct name of the ISP document in question. Alternatively, this potential pitfall can often be sidestepped by referring to specific actions (e.g., sharing passwords), rather than using abstract terms such as 'policy' or 'procedure'.

To illustrate the importance of this guideline, we offer an example from our research. We surveyed a hospital at which a key problem was that medical personnel left the patient records system freely accessible when they were away from the computer. Because of the sensitive nature of the information, this practice posed a liability risk to the hospital organization. On the basis of this problem, we developed a dependent variable that measured employees' practice of logging out of the patient records system. We validated this instrument with an expert panel composed of the hospital's information security manager, the CIO, IT staff of the hospital, IT consultants with experience with electronic patient systems, and medical doctors who did not belong to that hospital.

Unfortunately, we and the expert panel did not know that this particular patient records system offered the timesaving feature of quickly switching between simultaneously logged-in user accounts. Because of this feature, medical personnel at the hospital rarely logged out of the system, but instead locked the screen, allowing other users to access their accounts while protecting their own. Because our dependent variable did not match the organizational context, we could not accurately determine the extent of deliberate ISP violations involving the patient records system.

From this example, it is clear that determining whether a violation is common and important (Guideline 3) is not enough to make the study effective. Similarly, the use of previously validated instruments (Straub, 1989) is not enough. In addition to these steps, survey instrumentation must be validated for contextual relevance for respondents belonging to the target organization.

The best way to ensure that an instrument is contextually valid is to pretest the instrument with employees of the target organization. In addition to using a pretest to statistically test measurement validity (Straub *et al*, 2004), researchers should also ask employees for feedback about whether the instrument questions make sense in their context and whether scenarios (if used) are plausible or realistic in their situation. Without this, it would be

Table 3 Previous field surveys on ISP and security-related behavior in an organizational context

Study	*Objective(s) of the study*	*Guideline 1: States that a behavior is a violation of ISP*	*Guideline 2: Type of ISP violation (or behavior) is specified*	*Guideline 3: Practical relevance of the type of ISP violation is ensured*	*Guideline 4: Survey instrument pretested with target organization(s) for contextual validity*	*Guideline 5: Design Instrument for Appropriate Specificity and Generalizability*
Boss *et al* (2009)	Explain individual information security precaution-taking behavior using organizational control theory	No. The instrumentation measures IS security 'precautions taken', but does not indicate that this behavior involves an ISP violation	No. Survey items measure intention to comply at an abstract level, for example, 'I pay attention to computer security during my daily routine'. The justification to use generic measures is not discussed, they were taken from previous studies	N/A	No. They use students for the pretest, but do not report whether the survey instrument is validated for readability and applicability to the context of the respondents	No discussion of the appropriate level of specificity of the instrument
Bulgurcu *et al* (2010)	Use the theory of planned behavior to identify antecedents of employee compliance with the ISP of an organization	Yes. The instrumentation measures intentions to comply with the ISP	No. Survey items measure intention to comply at an abstract level, for example, 'I intend to comply with the requirements of the ISP of my organization in the future'. The justification to use generic measures is not discussed	N/A	No. They use a rigorous process for the development of instruments using faculty members and students, but they do not review the instruments with the target organization	No discussion on the appropriate level of specificity of the instrument. However, the use of generic measures is mentioned in the limitations section
Chan *et al* (2005)	Understand whether the information security climate influences employees' compliance with ISPs	Yes. The instrumentation measures intention to comply with ISP	No. Survey items measure intention to comply at an abstract level, for example, 'I will comply with information security procedures when performing my daily work'	N/A	No. The authors do not report how they have tested the survey instrument with the target organization	No discussion of the appropriate level of specificity of the instrument. While the stated objective is to measure 'core information security activities', it is unclear how the generic measures capture such activities
D'Arcy *et al* (2009)	Research how extended deterrence theory explains computer abuse	No. Scenarios describe IS misuse, but do not state that the behavior is an ISP violation	Yes. Scenarios are used to describe specific examples of possible violations, for example, fabricating payroll records	No. The scenarios were pretested for realism and content validity by 26 professionals. However, tests for the relevance of the scenarios to practice by information security managers or experts were not performed or were not reported	Yes. While they do not explicitly validate the instrument with the target organization, it can be concluded that the survey has been validated by people with a similar background	No discussion of the appropriate level of specificity of the instrument. However, the authors do vary the level of specificity used in the scenarios. Two scenarios are general, and one scenario is specific to context, and one is specific to a type of system
Guo *et al* (2011)	Present a combined model based on an extension to the theory of reasoned action and the theory of planned behavior	Yes. The scenarios state that an ISP violation is involved	Yes. Scenarios are used to describe specific examples of possible violations	No	No. The pretest sample consisted of employees from the university administration rather than the government organizations of the primary data collection	No discussion of the appropriate level of specificity of the instrument. The authors say they use 'specific scenarios'. Classified according to the rubric in Table 2, three are context-free, while one is specific to a type of system

Harrington (1996)	Study whether codes of ethics influence computer abuse intentions	No. Scenarios describe computer abuse, but do not state that the behavior is an ISP violation	Yes. Scenarios are used to describe specific examples of possible violations, for example, fabricating payroll records	No. Scenarios were adapted from previous studies. No tests for the relevance of the examples of computer abuse in the scenarios were reported	No. While the vignettes used by Harrington (1996) are based on previous studies, the instrument is tested with university students, not employees who could be seen to represent the respondents from the target population	No discussion of the appropriate level of specificity of the instrument. The scenarios used in this study are reported in Harrington (1992). All of the five scenarios are specific to a type of system
Herath & Rao (2009a)	Integrate protection motivation theory with the theory of reasoned action and formal sanctions in terms of deterrence theory	Yes. The instrumentation measures intentions to comply with ISP	No. Survey items measure intentions to comply at an abstract level, for example, 'I am likely to follow organizational security policies'	N/A	No. While Herath & Rao (2009a) use a rigorous process for validating the instrument by interviews using IS, computer science, and sociology scholars in addition to security experts, they do not review the instrument with employees belonging to the target population	No discussion of the appropriate level of specificity of the instrument. Items are taken from previous literature
Herath & Rao (2009b)	Study how penalties, pressures, and the perceived effectiveness of employees' actions influence the employees' ISP intentions	Yes. The instrumentation measures intentions to comply with ISP	No. Survey items measure intentions to comply at an abstract level, for example, 'I am likely to follow organizational security policies'	N/A	While Herath & Rao (2009a) use a rigorous process for validating the instrument by interviews using IS, computer science, and sociology scholars in addition to security experts, they do not review the instrument with employees belonging to the target population	No discussion of the appropriate level of specificity of the instrument. Items are taken from previous literature
Hu *et al* (2011)	Examine whether sanctions actually deter employees' noncompliance with ISP	No. Scenarios describe IS misuse, but do not state that the behavior is an ISP violation	Yes. Scenarios are used to describe specific examples of possible violations	No	No. They use students for pilot tests, but they do not report any tests or interviews in which the target population (employees) is used to test the validity of the instrument. However, the applicability of the dependent variable is checked, in that a validation question was included after each scenario, which asks the respondents about how likely the scenarios would be in their companies	No discussion of the appropriate level of specificity of the instrument. The scenarios used in this study are reported in Hu *et al* (2010). All of the three scenarios are specific to a type of system
Johnston & Warkentin (2010a)	Investigate the influence of fear appeals on the compliance of end-users with recommendations to use anti-spyware software	N/A	No. Survey items measure intentions to comply at an abstract level, for example, 'I intend to use anti-spyware software in the next 3 months'	N/A	They use faculty members and students to ensure content validity but do not report any details of the process. The use of students and faculty members for the purpose of reviewing the instrument for understandability and applicability would meet Guideline 4 in the sense that they use same population for the actual data collection	While they do not discuss the appropriate level of specificity of the instrument, they explicitly state that their study findings should be generalizable to all decentralized environments where users exercise autonomous control. Measurement items capturing the dependent variable are at the context-free level of specificity

Table 3 Continued

Study	*Objective(s) of the study*	*Guideline 1: States that a behavior is a violation of ISP*	*Guideline 2: Type of ISP violation (or behavior) is specified*	*Guideline 3: Practical relevance of the type of ISP violation is ensured*	*Guideline 4: Survey instrument pretested with target organization(s) for contextual validity*	*Guideline 5: Design Instrument for Appropriate Specificity and Generalizability*
Johnston & Warkentin (2010b)	Examine the effect of perceived source credibility on end-user attitudes and intentions to comply with recommended actions to avert spyware	N/A	No. Survey items measure intentions to comply at an abstract level, for example, 'I intend to use anti-spyware software in the next 3 months'	N/A	They use faculty members and students to ensure contextual validity but do not report any details of the process. The use of students and faculty members for the purpose of reviewing the instrument for understandability and applicability would meet Guideline 4 in the sense that they use same population for the actual data collection	Measurement items capturing the dependent variable are at the context-free level of specificity
Lee *et al* (2004)	Study how security policy, training, and trust deter computer abuse	No. The survey instrument measures intentions to commit computer abuse, but does not state that this is a violation of policy	Yes. Survey items measure several examples of computer abuse, for example, intention to use another person's ID without authorization	No. No tests for relevance of the examples of computer abuse in the instrumentation were reported	No. They use part-time M.B.A. students for a pilot study, but do not report whether they have reviewed the instrument for understandability and applicability using the same population as in the actual data collection	No discussion of the appropriate level of specificity of the instrument Measurement items capturing the dependent variable vary between generic and context-free levels of specificity
Myyry *et al* (2009)	Investigate whether Kohlberg's theory of moral decision making explains one's intentions to share passwords	No. The scenario used does not specify that the behavior was a violation of ISP	Yes. The scenario describes a specific example of possible violations, for example, sharing a password with others	No. No tests for relevance of the examples of computer abuse in the instrumentation were reported	No. They use a pilot test for testing the validity, but do not report whether they have reviewed the instrument for understandability and applicability using the same population as in the actual data collection	No discussion of the appropriate level of specificity of the instrument. Measurement items capturing the dependent variable are specific to a context and to a type of system
Ng *et al* (2009)	Investigate how the health belief model explains secure email practices	No. The survey instrument measures computer security intentions, but does not state that this is a violation of policy	Yes. Survey items measure several examples of computer security behaviors, for example, 'Before reading an email, I will first check if the subject and the sender make sense'	No. Pretests of items were performed with experts in the field. However, no tests for the relevance of the examples of information security behaviors were reported	No. Pretests of items were performed with experts in the field. However, the researchers did not report using the target population to test the validity of the instrument	No discussion of the appropriate level of specificity of the instrument. Measurement items capturing the dependent variable are specific to a context and to a type of system
Pahnila *et al* (2007)	Create a model combining protection motivation theory, the theory of reasoned action, habit, deterrence theory, and innovation diffusion theory	Yes. The survey instrument measures intentions to comply and actual compliance	No. Survey items measure intentions to comply at an abstract level	N/A	No	No discussion of the appropriate level of specificity of the instrument. Instrumentation not reported

	Study how protection motivation theory rewards and deterrence explains employees' compliance with ISPs	Yes. The survey instrument measures intentions to comply	No. Survey items measure intentions to comply at an abstract level	N/A	No. They reviewed the instrument with 15 people, but the researchers did not report using the target population to test the validity of the instrument	No discussion of the appropriate level of specificity of the instrument. Instrumentation not reported
Siponen & Vance (2010	Research how neutralization techniques influence employees' compliance with ISPs	Yes. The scenarios state that an ISP violation is involved	Yes. The scenarios give specific examples of ISP violations	Yes. A total of 54 information security professionals were polled to determine the most important ISP violations	No. They pretested their instrument with a panel of experts and employees at two organizations, but did not report whether they pretested the instrument with employees of the target organizations. The realism of scenarios was checked, in that respondents were asked to report if they found the scenarios realistic	They discuss the need to add context details to the scenarios, but the appropriate level of specificity is not discussed. The level of specificity of the scenarios varies from specific to violation to specific to context. No explanation is given for the varying levels of specificity
Siponen *et al* (2010)	Investigate how protection motivation theory explains employees' compliance with ISPs	Yes. The survey instrument measures intentions to comply and actual compliance	No. Survey items measure intention to comply at an abstract level	N/A	No	No discussion of the appropriate level of specificity of the instrument. Instrumentation not reported
Son (2011)	Understand the influence of intrinsic and extrinsic motivation on employees' compliance with ISPs	Yes. The instrumentation measures self-reported compliance with ISPs	No. Survey items measure compliance with five different general categories of ISP behaviors that form a formative construct of 'compliance'. However, each category is defined at a high level (e.g., 'I comply with information systems security policy (ISSP) with regard to use of the Internet and network resources')	No. Pretests of items were performed with IS faculty members with experience in survey-based research. However, no tests for the relevance of the examples of information security behaviors were reported	No	No discussion on the appropriate level of specificity of the instrument
Straub (1990)	Study how formal sanctions in terms of the deterrence theory deter computer abuse	No. The survey measured computer abuse, but did not specify a violation of ISP	No. General objective measures of computer abuse were used (e.g., the number of incidents and the actual dollar loss)	N/A	Straub uses many interviews with different people, including CIOs, to validate the survey instrument. This matches the target population in the sense that Straub (1990) is surveying not employees' perceptions, but the perceptions of the CIO and the managers	N/A. General objective measures of computer abuse were used, for example, the number of incidents and the actual dollar loss. The items for this study are reported in Straub (1989)

difficult to obtain an accurate understanding of deliberate ISP violations.

Guideline 5: consider the appropriate level of specificity and generalizability for instrumentation

The level of specificity of the measures of a survey instrument has implications for generalizability, which is an important concern in scientific research (Lee & Baskerville, 2003; Burton-Jones *et al*, 2012). In order to illustrate what we mean by level of specificity, Table 2 illustrates four levels of specificity. Generalizability means that a knowledge claim supported in one context holds in other contexts as well (Seddon & Scheepers, 2011). By generalizability, we refer to sampling-based generalizability, which only applies to quantitative studies, such as variance models (Lee & Baskerville, 2003).

Simply summarized, sampling-based generalizability means that a theory or model can be generalizable to different (A) organizations, (B) cultures/countries, and (C) behaviors. Applied to ISP violations, this means that a theory that explains more than one type of IS security behavior is more generalizable in terms of behavior (C) than a theory that explains only one type of behavior. Similarly, a theory that explains phenomena in more than one organization is more generalizable in terms of applicability to different organizations (A) than a theory that explains the phenomena in just one organization. Finally, the same is true of theories that generalize in terms of cultures and countries (B).

In the case of variance models, it is important to determine how generalizable a theory is in terms of A, B, and C and also to design the instrument in a way in which assumptions about generalizability are explicitly considered. This means that one cannot claim that one type of generalizability is more generalizable than the others. For example, Theory 1 may be more generalizable in terms of culture than Theory 2, but the opposite may be true in terms of the generalizability of behaviors. Hence, theoretically speaking, all four types presented in Table 2 could be generalizable across countries and cultures.

In terms of behavior, ‘I use easy-to-guess passwords for work systems’ (specific to context, Table 2) is potentially more generalizable in terms of behaviors than ‘I use easy-to-guess passwords for Human Resource Systems’ (specific to type of system, Table 2). The ‘context-free specification of violations’ level (Table 2) assumes behavioral generalizability across different contexts and domains. This level of specificity (I use easy-to-guess passwords) is suitable for studies that assume that ISP violations do not differ from one context or systems to another, or studies whose theory explains all kinds of non-compliance behaviors.

The ‘specific to context’ level could be used when authors assume that the context is a boundary condition. For example, theory could suggest that employees adopt different security behaviors in the work context than they do in the home. Similarly, the ‘specific to type of system’ would suggest that the type of the system is the boundary condition. For example, employees may use strong passwords for a banking application, but weaker passwords for less important systems.

Here we do not want to limit the theory development by preferring any of these types of level of specificity. Instead, we urge scholars to explicitly consider what the appropriate level of specificity is for their study. While this decision relates to generalizability, it also depends on theoretical assumptions about boundary conditions (e.g., whether a security behaviors differ across work and home contexts).

Increasing generalizability when using specific measures

The guideline for specifying the characteristics of a situation, as suggested by Guideline 2, does not necessarily decrease the generalizability of research results. Indeed, specific measures can also be generalizable. For example, the item ‘I use easy-to-guess passwords’ (specified in Table 2) is potentially more generalizable in terms of behaviors than ‘I use easy-to-guess passwords for human resource systems’ (specific to systems and certain types of systems, Table 2) because the former refers to any work system, not just human resource systems.

However, generalizability can be increased when using specific measures by employing the following techniques. First, scholars can prepare different versions of the survey instrument to measure a variety of security behaviors. For example, half of the respondents could receive items measuring password behavior, and the other half could receive measures relating to locking the workstation screen. In this way, the scholars can demonstrate the generalizability of their theory by showing that their results are consistent across different behaviors.

Second, a similar approach can be taken with scenario-based instruments. Respondents can rate multiple scenarios describing different ISP violations (e.g., D’Arcy *et al*, 2009), or respondents can randomly receive different scenarios to rate (e.g., Siponen & Vance, 2010; Hu *et al*, 2011). If the theoretical variables predict the dependent variable across all the types of ISP violations described in the different scenarios then this is strong evidence that the theory can be generalized across behaviors.

Third, the factorial survey method can be used to randomly vary the type as well as the specificity of the ISP violation described in the scenario. The factorial survey method is a powerful means of determining which contextual details of a scenario are more relevant in influencing intentions or judgments (Rossi, 1979; Jasso, 2006). For example, in Paternoster & Simpson (1996), not only was the type of scenario varied, but also contextual details embedded in the scenario were varied. A similar approach may be taken to vary the specificity of details in the scenario.

How previous IS security behavior research meets the five guidelines

Next, we consider previous studies on IS security behavior in the context of the five guidelines we have

Table 4 Five guidelines at a general level of abstraction

Guidelines	*Descriptions*
Guideline 1: Ensure that respondents recognize the phenomenon of interest in the instrumentation	Ensure that you truly specify the phenomenon and its boundaries in the instrumentation so that respondents accurately perceive the phenomenon
Guideline 2: Measure the phenomenon concretely	Measurements of intentions or behavior should be measured concretely, as appropriate for the research phenomenon
Guideline 3: Ensure that the dependent variable focuses on important problems in practice	Elicit input from practitioners to ensure that the dependent variable is relevant and important to problems in practice. When eliciting input from practitioners, exercise careful consideration as to what type of employee is most capable of providing insights into the phenomenon of interest
Guideline 4: Ensure the applicability of instrumentation to respondents' organizational context	Ensure that the instrumentation is applicable to the organizational context of respondents. This requires in-depth knowledge of the target environment, including the correct terminology that organizational members use. Survey items drawn from previously validated instruments may not be applicable or have different meanings to respondents of the target organization
Guideline 5: Theorize the appropriate level of specificity and generalizability for instrumentation	Determine the appropriate level of specificity for the research study. This depends on theoretical assumptions about boundary conditions of the theory

outlined. In fairness, the majority of these studies were not designed or intended to study deliberate violations of ISPs. Our purpose in making this comparison is not to criticize previous work, but rather to clearly highlight the gap in our understanding of deliberate violations of ISPs.

Table 3 describes previous studies and the extent to which they meet our five guidelines. It should be noted that studies that do not specify the type of violation (Guideline 2) necessarily do not meet the guideline for relevance of the violation (Guideline 3). This is because studies that do not specify the type of violation cannot ensure that the type of violation is also relevant. Studies in this category include Bulgurcu *et al* (2010), Chan *et al* (2005), Herath & Rao (2009a, b), Johnston & Warkentin (2010a), Lee *et al* (2004), Pahnila *et al* (2007), Siponen *et al* (2007), Siponen *et al* (2010), and Straub (1990). These are classified in Table 3 as 'not applicable' (N/A) with respect to Guideline 3.

The scope of our review was such that only empirical survey studies (1) on behavioral issues in IS security (2) in an organizational context (3) that were published between 1990 and 2011 were included. Thus, we did not review papers such as Anderson & Agarwal (2010), who examined the security behavior of individual users.

As can be seen from Table 3, seven studies specify specific violations (Harrington, 1996; Lee *et al*, 2004; Ng *et al*, 2009; D'Arcy *et al*, 2009;Myyry *et al,* 2009; Guo *et al,* 2011; Hu *et al,* 2011) and seven more study deliberate violations of ISPs (Chan *et al,* 2005; Pahnila *et al,* 2007; Siponen *et al,* 2007; Herath & Rao, 2009a, b; Siponen *et al,* 2006; Bulgurcu *et al,* 2010). However, only two (Siponen & Vance, 2010; Guo *et al,* 2011) meet both Guidelines 1 and 2. In addition, only one study (Siponen & Vance, 2010) meets Guideline 3, which ensures that the authors study relevant and important problems in the practice of information security management.

Only three studies (Straub, 1990; D'Arcy *et al*, 2009; and possibly Johnston & Warkentin, 2010a) meet the fourth guideline, which suggests that the survey instrument (items and scenarios, if any) must be validated with the target population of the survey in order to ensure the applicability of the instrument to the organizational context. While D'Arcy *et al* (2009) do not explicitly validate the instrument with the target population, it can be concluded that the survey was validated with people of similar background. Hence, the study meets Guideline 4. No study explicitly discusses Guideline 5.

Regarding studies specifying the type of violation (Guideline 1), Myyry *et al* (2009) use a specific scenario, but do not report how the relevance of the scenario was validated. Similarly, Ng *et al* (2009) do not report whether the types of violations were tested for relevance. Harrington (1996) uses vignettes from previous research, but neither Harrington (1996) nor the previous studies from which the scenarios were drawn report whether the scenarios were validated for relevance. In contrast, D'Arcy *et al* (2009) did pretest their instrument with a group of 26 working professionals taking M.B.A. classes, but they did not state whether the professionals had expertise in information security nor did they indicate how the practical relevance of the scenarios was tested.

Please note that this does not mean that these studies are not practically relevant; rather, these studies have not expressly *ensured* or *validated* the practical relevance of the phenomenon studied. For example, a study that uses a panel of IS security practitioners and subject experts merely to validate the content of a scenario involving an ISP violation does not meet Guideline 3. However, if the same panel were also specifically asked whether the scenario represented an important and common violation of ISP, the study would meet Guideline 3. This is because the second example validates or ensures the practical relevance of the violation, whereas the first does not.

A related problem is to have the scenario validated by a panel of professionals without security expertise or experience (e.g., D'Arcy, *et al* 2009). As argued earlier, the practical relevance of the ISP violations should be tested with security managers or subject experts, instead of or in addition to non-security professionals such as students, general IT professionals, or regular employees. While non-security professionals may be able to identify whether a violation is common, they lack the expertise to judge whether a violation is also important or a key problem for an organization.

Guideline 4 suggests that the survey instrument (items and scenarios, if used) must be validated with the target population of the survey in order to ensure the applicability of the instrument to the organizational context. Three studies (Straub, 1990; D'Arcy *et al*, 2009; and possibly Johnston & Warkentin, 2010a) meet this guideline. For example, D'Arcy *et al* (2009) tested the survey with professionals and faculty members for validity and clarity. While the exact details are not reported and they do not explicitly validate the instrument with the target organization, it can be concluded that the survey has been tested for readability and applicability by people with a similar background.

Finally, Guideline 5 suggested that studies should consider what the appropriate level of specificity should be in measuring the dependent variable. As can be concluded from Table 2, different studies use different levels of specificity, and some studies even vary in the level of specificity for different scenarios without explanation. However, most of the studies do not consider the level of specificity. Siponen & Vance (2010) provide justification for adding contextual details to their scenarios, but they do not justify why they chose to use varying levels of specificity. Only Johnston & Warkentin (2010a) explicitly state that their study findings should be generalizable to all decentralized environments where users exercise autonomous control. However, as with all other studies we examined, they do not discuss the appropriate level of specificity for their instrument.

Discussion

We propose five guidelines to increase the practical applicability of field survey research using employees' deliberate ISP violations as an example. We then compared the five guidelines against existing behavioral survey research on information security and found that most studies meet two or fewer of the guidelines and that no study meets more than three. These findings show that while our knowledge of behavioral IS security issues is increasing there is a need to improve research design and make certain decisions more explicit. While our guidelines are specific to ISP violations, they are easily generalizable to field surveys in other areas of IS research. We next offer our guidelines in general form in Table 4 and discuss their application.

Guideline 1 may be more generally stated as 'ensure that respondents recognize the phenomenon of interest in the instrumentation'. Consider the widely studied area of software piracy (Siponen *et al,* 2012). In such a context, it makes a great deal of difference that respondents recognize whether or not copying software violates the terms of the software license. If software piracy intentions are the phenomenon under investigation, then the instrumentation should make clear to respondents that they are reporting their intention to pirate software. Otherwise, researchers may capture intentions to legally copy software, which could in turn confound the results.

Guideline 2 can be restated as 'measure the phenomenon concretely'. This means that scholars should specify the phenomenon they study unambiguously, being cognizant that how they operationalize the items may make a difference. To illustrate this in the context of IT use, it may make a difference whether intention to use is asked in an unspecific manner (e.g., 'I intend to use a system') as compared with the type of use specified (e.g., 'I intend to use games,' or 'I intend to use an email client'). For example, a model might have significantly different results if the dependent variable is measured as 'I intend to use a system' rather than 'I intend to use games'. Thus, in this example, the instrumentation should specify the technology.

We generalize Guideline 3 as 'ensure that the dependent variable focuses on an important problem in practice'. This guideline is foundational to applied science in the sense that in applied science scholars need to solve (or increase understanding of) practical problems. Before developing instrumentation, researchers should validate that the phenomenon of interest is an important issue for practitioners. For example, a growing area of research is health information technology (HIT) (Romanow *et al,* 2012). Applying Guideline 3, a researcher could interview or otherwise interact with experienced healthcare practitioners to verify that the phenomenon to be studied is actually a pressing problem for HIT practice. While there are other methods to verify practical relevance (e.g., conducting a literature review of practitioner literature), it is helpful to have a practitioner 'on the ground' who is struggling with current issues to inform the selection of the phenomenon to study. Following this approach increases the likelihood that the research will have an impact on practice. In addressing this issue, the scholars should not take the shortcut of finding the most convenient practitioner to interview. Rather, the key lies in understanding which type of practitioner is most qualified to inform the research.

The generic version of Guideline 4 is to 'ensure the applicability of instrumentation to respondents' organizational context'. Ensuring the applicability of instrumentation to the respondents' organizational context requires in-depth knowledge about the target environment, including the correct terminology that respondents use. A typical problem is that while survey questions may be based on previously validated questions the terms may not be understandable to the respondents, or respondents may understand the terms differently than the researchers do. An example of this is software development. It is common that software developers modify textbook methods based on their experience, mix them with other software development methods, and omit certain stages (Abrahamsson *et al,* 2003; Siponen & Iivari, 2006). If that is the case, asking questions about a method using its textbook name could confuse or mislead respondents.

Finally, Guideline 5 can be restated as 'theorize the appropriate level of specificity and generalizability for instrumentation'. Levels of specificity range from context-free specification (I intend to use a system), specific to context (I intend to use a work system), specific to a type of system, (I use easy-to-guess passwords for human resource systems), and specific to a particular system (I intend to use Facebook). Applying this guideline depends on theoretical assumptions about boundary conditions of the theory that scholars apply (see Guideline 5). In other words, scholars need to consider what is the most appropriate level of specificity based on their theoretical assumptions.

Our purpose in explicating these five guidelines is to make IS scholars aware of some of the key issues that are relevant in ensuring the practical relevance of the survey research, using employees' deliberate ISP violations as an example. By explicating these issues, IS scholars can make informed decisions about how these five issues should be addressed in their research.

Limitations of the guidelines

Our five guidelines have limitations. First, it must be noted that our guidelines are not intended to be exhaustive. Rather, they are designed to highlight five important, yet easy to overlook, research issues regarding employees' deliberate violations of IS security policies.

Second, while ensuring that practical relevance is important there are problems if practical relevance is taken to an extreme. This means that Guideline 3 (Ensure that the dependent variable focuses on important problems in practice) should not be interpreted to suggest that practice should dictate research issues. Sometimes it is justifiable to research a given topic even if it is not in vogue in practice. This is because practitioners, with their focus on day-to-day activities, may not recognize some relevant long-term issues on the horizon that may be apparent to a scholar with a wider research perspective.

Third, the guidelines are based on the assumption that examinations of ISP violations are conducted within the paradigm of applied science, in which practical relevance is valued. Hence, our guidelines are not suited to being observed under the assumptions of basic science, in which practical applicability is not a chief consideration. While IS is regarded as an applied field (Benbasat & Zmud, 1999) and we believe in ensuring practical relevance without sacrificing rigor, it is also important to recognize the role of basic research, in which the aim is to search for truth or truthlikeness for its own sake, without having any practical applications in mind.

Conclusions

We argue that applied IS survey research, aimed at tackling practical problems, needs to ensure contextual-level relevance. While the importance of contextual relevance may appear self-evident, we find that the current discussion and practice of contextual relevance in IS research is unsatisfactory. We argued that the content of the instrument may be rigorously validated and yet be out of touch with practice. In this opinion article, we outlined five guidelines – relating to both rigor and relevance – designed to increase the practical applicability of field survey research. We used the problem domain of ISP violations to instantiate our guidelines. Given the increased use of IT in the workplace and the fact that sensitive, work-related information is increasingly stored ubiquitously on mobile devices, employees' compliance with ISPs is becoming a progressively important issue for organizations.

The first of our guidelines is that respondents need to be informed that the act in question is a violation of an ISP. Second, studies focusing on employees' intentional violation of ISPs should measure specific examples of violations. Third, studies focusing on employees' intentional violations of ISPs should ensure that the examples of violations studied are relevant and important problems in practice. Fourth, the applicability of the survey instrumentation describing the ISP violation should be contextually valid for the target organization. Fifth, the level of specificity and generalizability should be appropriate for the selected theory and its assumed boundary conditions. We demonstrated that in the IS security behavior literature most studies meet two or fewer of these guidelines.

Finally, we generalized our guidelines for application to field surveys in IS research general. Our purpose in explicating these five guidelines is to encourage IS scholars to make carefully considered decisions about how they should address these issues in their research. Such decisions should go beyond appealing to previous research conventions. They may also be helpful for reviewers and editors as they evaluate field surveys on ISP violations and IS in general. By applying these guidelines, we believe that scholars will enhance the rigor of their work and obtain highly relevant results for important problems in practice.

Acknowledgements

We wish to thank the AE Merrill Warkentin for his extensive guidance throughout the review process. We also thank several anonymous reviewers for their helpful comments. Finally, we thank the Finnish Funding Agency for Technology and Innovation for funding this research.

About the Authors

Mikko Siponen holds positions of Professor at the University of Jyväskylä and the University of Oulu, in Finland. He is the Director of the IS Security Research Centre in the Department of Information Processing Science at the University of Oulu. He holds Ph.D.s in philosophy from the University of Joensuu; and information systems, from the University of Oulu. He has published in outlets such as *MIS Quarterly, Journal of the Association for Information Systems*, and *European Journal of Information Systems*.

Anthony Vance is as an Assistant Professor of Information Systems in the Marriott School of Management of Brigham Young University. He has earned Ph.D. degrees in Information Systems from Georgia State University, U.S.A.; the University of Paris Dauphine, France; and the University of Oulu, Finland. His work is published in outlets such as *MIS Quarterly, Journal of Management Information Systems*, and *European Journal of Information Systems*. His research interests are information security and trust in information systems.

References

Abrahamsson P, Warsta J, Siponen MT and Ronkainen J (2003) New directions on agile methods: a comparative analysis. *Software Engineering*, Proceedings of the 25th International Conference on IEEE. IEEE, Portland, OR, pp. 244–254.

Aftab P (2003) The privacy lawyer: cyberloafing's drain on productivity. *Information Week*, [WWW document], http://www.informationweek.com/news/16000567.

Akers RL and Sellers CS (2004) *Criminological Theories: Introduction, Evaluation, and Application*, 4th edn. Roxbury Press, Los Angeles.

Alexander CS and Becker HJ (1978) The use of vignettes in survey research. *Public Opinion Quarterly* **42(1)**, 93–104.

Anderson C and Agarwal R (2010) Practicing safe computing: a multimethod empirical examination of home computer user security behavior intentions. *MIS Quarterly* **34(3)**, 613–643.

Bachman R, Paternoster R and Ward S (1992) The rationality of sexual offending: testing a deterrence/rational choice conception of sexual assault. *Law & Society Review* **26(2)**, 343–372.

Benbasat I and Zmud R (1999) Empirical research in information systems: the practice of relevance. *MIS Quarterly* **23(1)**, 3–16.

Boss S, Kirsch L, Angermeier I, Shingler R and Boss R (2009) If someone is watching, i'll do what i'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* **18(2)**, 151–164.

Boudreau M, Gefen D and Straub DW (2001) Validation in information systems research: a state of-the-art assessment. *MIS Quarterly* **25(1)**, 1–26.

Bulgurcu B, Cavusoglu H and Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* **34(3)**, 523–548.

Burton-Jones A, McLean E and Monod E (2012) On approaches to building theories: process, variance and systems. Working Paper.

Bush V (1945) *Science – the Endless Frontier: A Report to the President*. U.S. Government Printing Office, Washington DC.

Chan M, Woon I and Kankanhalli A (2005) Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security* **1(3)**, 18–41.

Clarke R and Felson M (1993) Criminology, routine activity and rational choice. In *Routine Activity and Rational Choice* (Clarke R and Felson M, Eds), pp. 1–14, Transaction Publishers, New Brunswick, NJ.

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* **20(1)**, 79–98.

Ernst and Young (2008) Ernst & Young 2008 global information security survey. [WWW document], http://www.ey.nl/download/publicatie/2008_GISS_rapport_DEF__1.pdf (accessed 31 May 2010).

Guo K, Yufei Y, Archer N and Connelly C (2011) Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems* **28(2)**, 203–236.

Harrington SJ (1992) The characteristics and ethical judgments of members of the computer profession: a behavioral model. Dissertation, Kent State University.

Harrington SJ (1996) The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly* **20(3)**, 257–278.

Herath T and Rao HR (2009a) Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems* **18(2)**, 106–125.

Herath T and Rao HR (2009b) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems* **47(2)**, 54–165.

Hu Q, Xu Z, Dinev T and Ling H (2010) The centrality of low self-control in internal computer offenses. In *Proceedings of the Dewald Roode Information Security Research Workshop* (Vance A, Ed), (sponsored by IFIP WG8.11/WG11.13) Bentley University, Waltham, MA.

Hu Q, Xu Z, Dinev T and Ling H (2011) Does deterrence really work in reducing information security policy violations by employees? *Communications of the ACM* **54(6)**, 54–60.

Hui C and Triandis H (1985) Measurement in cross-cultural psychology: a review and comparison of strategies. *Journal of Cross-Cultural Psychology* **16(2)**, 131–152.

Jasso G (2006) Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research* **34(3)**, 334–423.

Johnston A and Warkentin M (2010a) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* **34(3)**, 549–566.

Johnston A and Warkentin M (2010b) The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational and End User Computing* **22(3)**, 1–21.

Karjalainen M and Siponen M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems* **12(8)**, Article 3.

Klepper S and Nagin D (1989) The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology* **27(4)**, 721–746.

Klockars CB (1974) *The Professional Fence*. Free Press, New York.

Lee A and Baskerville R (2003) Generalizing generalizability in information systems research. *Information Systems Research* **14(3)**, 221–243.

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

Limayem M and Hirt SG (2003) Force of habit and information systems usage: theory and initial validation. *Journal of the AIS* **4(1)**, 65–97.

Mackenzie SB, Podsakoff PM and Podsakoff NP (2011) Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. *MIS Quarterly* **35(2)**, 293–334.

McGrath J (1981) Dilemmatics: the study of research choices and dilemmas. *American Behavioral Scientist* **25(2)**, 179–210.

Moore G and Benbasat I (1991) Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research* **2(3)**, 192–222.

Myyry L, Siponen M, Pahnila S, Vartiainen T and Vance A (2009) What levels of moral reasoning and values explain adherence to information security policies? An empirical study. *European Journal of Information Systems* **18(2)**, 126–139.

Ng BY, Kankanhalli A and Xu Y (2009) Studying users' computer security behavior using the health belief model. *Decision Support Systems* **46(4),** 815–825.

Niiniluoto I (1993) The aim and structure of applied research. *Erkenntnis* **38(1),** 1–21.

O'Fallon M and Butterfield K (2005) A review of the empirical ethical decision-making literature: 1996–2003. *Journal of Business Ethics* **59(4),** 375–413.

Pahnila S, Siponen M and Mahmood A (2007) Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. Los Alamitos, CA, IEEE Computer Society Press, pp. 156–166.

Parker D (1976) *Crime by Computer*. Scribner, New York.

Petter S, Straub D and Rai A (2007) Specifying formative constructs in IS research. *MIS Quarterly* **31(4),** 623–656.

Paternoster R and Simpson S (1996) Sanction threats and appeals to morality: testing a rational choice model of corporate crime. *Law and Society Review* **30(3),** 549–584.

Piquero NL, Exum ML and Simpson SS (2005) Integrating the desire-for-control and rational choice in a corporate crime context. *Justice Quarterly* **22(2),** 252–280.

PricewaterhouseCoopers (2010) Information security breaches survey 2010. [WWW document], http://www.pwc.co.uk/pdf/isbs_survey_2010_technical_report.pdf (accessed 31 May 2010).

Puhakainen P and Siponen M (2010) Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly* **34(4),** 757–778.

Robinson S and Bennett R (1995) A typology of deviant workplace behaviors: a multidimensional scaling study. *Academy of Management Journal* **38(2),** 555–572.

Romanow D, Cho S and Straub D (2012) Riding the wave: past trends and future directions for health IT research. *MIS Quarterly* **36(3),** iii–x.

Rossi P (1979) Vignette analysis: uncovering the normative structure of complex judgments. In (Robert KM, James SC and Peter HR Eds) *Qualitative and Quantitative Social Research: Papers in honor of Paul F. Lazarsfeld*, pp. 176–186, Free Press, New York.

Seddon P and Scheepers R (2011) Towards the improved treatment of generalization of knowledge claims in IS research: drawing general conclusions from samples. *European Journal of Information Systems* **21(1),** 6–21.

Siponen M, Baskerville R and Heikka J (2006) A design theory for secure information systems design methods. *Journal of the Association for Information Systems* **7(11),** 725–770.

Siponen MT (2000) A conceptual foundation for organizational IS security awareness. *Information Management & Computer Security* **8(1),** 31–41.

Siponen MT and Iivari J (2006) IS security design theory framework and six approaches to the application of ISPs and guidelines. *Journal of the Association for Information Systems* **7(7),** 445–472.

Siponen MT, Mahmood A and Pahnila S (2010) Why employees don't comply with information security policies: an empirical investigation. *IEEE Computer* **43(10),** 64–71.

Siponen MT and Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* **34(3),** 487–502.

Siponen MT, Vance A and Willison R (2012) New insights into the problem of software piracy: the effects of neutralization, shame, and moral beliefs. *Information & Management* **49(7–8),** 334–341.

Son J (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management* **48(7),** 296–302.

Stafford T (2011) Special research commentary series on advanced methodological thinking for quantitative research. *MIS Quarterly* **35(2),** xv–xvi.

Stanton J, Stam K, Mastrangelo P and Jolton J (2005) Analysis of end user security behaviors. *Computers and Security* **24(2),** 124–133.

Stokes D (1997) *Pasteur's Quadrant: Basic Science and Technological Innovation*. Brookings Institutional Press, Washington DC.

Straub DW (1989) Validating instruments in MIS research. *MIS Quarterly* **13(2),** 147–169.

Straub DW (1990) Effective IS security: an empirical study. *Information Systems Research* **1(3),** 255–276.

Straub DW and Ang S (2011) Rigor and relevance in IS research: redefining the debate and a call for future research. *MIS Quarterly* **35(1),** iii–xi.

Straub DW, Boudreau M and Gefen D (2004) Validation guidelines for IS positivist research. *Communications of the AIS* **13(24),** 380–427.

Tijssen R (2010) Discarding the 'basic science/applied science' dichotomy: a knowledge utilization triangle classification system of research journals. *Journal of the American Society for Information Science and Technology* **61(9),** 1842–1852.

Trevino LK (1992) Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly* **2(2),** 121–136.

Weir C (2005) Limitations of the common European framework for developing comparable examinations and tests. *Language Testing* **22(3),** 281–300.

Willison R and Warkentin M (2013) Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly* **37(1),** forthcoming.