Journal of the Association for Information Systems (2018) **19**(4), 247-265
doi: 10.17705/1jais.00491

EDITORIAL

ISSN 1536-9323

Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example

Mikko Siponen[1] and Richard Baskerville[2]

[1]Faculty of Information Technology, University of Jyväskylä, Finland, mikko.t.siponen@jyu.fi
[2]Georgia State University, USA, and Curtin University, Australia, baskerville@acm.org

Abstract

In the current information systems security (ISS) research, new theory contributions are especially valued. This research typically reflects the following formula: Suggest a new theory (or set of constructs) of ISS and show that it is empirically supported, then suggest another new theory (or set of constructs with some linkages) and show that it is empirically supported, and so on. Despite the merits of this approach, it leaves out many important scientific aspects. For example, after more than 30 years of ISS research, (1) we know little about the conditions and situations to which new theories (or constructs) do not apply; (2) we do not know which new theories are more effective than others in solving an ISS problem; and (3) we have not demonstrated that our best research, or new theoretical contributions, can beat industry best practices or practitioners' intuitive approaches. We suggest that ISS research be examined in terms of long-term research programs comprising four levels: metalevel research, basic research, applied research, and postintervention research. The ultimate success of such programs does not entail new theories, "contextualized theories," or adding IT artifacts to theories; rather, it hinges on the question of which program can demonstrate the best intervention effect rate for a given ISS problem. The lack of demonstrated intervention effectiveness (e.g., by showing treatment effect rates) is one important inhibitor that may prevent ISS research from achieving relevance in practice. Without reporting such evidence, ISS research cannot overpower the folklore, fads, or industry "best practices" that often guide operations. With such treatment effect rates, evidence-based practice may become more justifiable. We believe that our ideas also can be applied to information systems research in general.

Keywords: Practical Relevance, IS Security, Intervention Effect, History of IS Security.

Suprateek Sarker was the accepting senior editor for this editorial.

1 Introduction

In the information systems (IS) discipline, there has been awareness of the lack of sufficient relevance to practice (Alter 2001; Benbasat & Zmud, 1999; Keen 1991; Robey & Markus, 1998; Rosemann & Vessey, 2008). An important aspect of practical relevance, which has not been clearly articulated in previous IS research, is demonstrating the rate of application effectiveness. This can be demonstrated, for example, by indicating the intervention effect. Applying IS research to information security management as an example, we show how improved reporting of intervention effect rates offers additional important steps toward achieving practical relevance and acceptability of research in practice. An *intervention* (or *treatment*) *effect rate* refers to the degree to which the essential practical problem underlying the research is reduced following intervention or treatment. Intervention/treatment effect rates are more stringent measures than having practitioners evaluate research results (e.g., "applicability checks"; Rosemann & Vessey, 2008) because the effects of the research products on the practical problem must be identifiable.

Providing such research results could bring the IS research community closer to *guiding* and *leading* practice. The example of information systems security (ISS) management illustrates the serious gap in effective IS management practice, which is open to IS research for guidance and contributions.

The gravity of the gap in practical ISS management knowledge is most apparent in the near-daily reports of ISS and privacy breaches. The ISS problem is huge, with the worldwide average cost per data breach estimated to be between $2.5 million (PwC, 2016) and $4 million (Ponemon Institute, 2016). Verizon's 2016 survey of law enforcement agencies disclosed 64,199 reported breaches with 2,260 confirmed cases of data losses. In addition to costing organizations millions, these security lapses harm millions of people directly. For example, the number of U.S. individuals' private records exposed since 2005 totals over 900 million (over 160 million in 2015 alone) (Privacy Rights Clearinghouse, 2016). Thus, the ethical pressures on security professionals (and researchers) to reduce these losses are vast.

This practical problem has grown so rapidly that ISS management practice is struggling to keep pace, much less get ahead of the problem. We suggest that increasing our expectations of more exhaustive ISS research would help—particularly in terms of expectations that such research should lead to more reporting of intervention/treatment effect rates.

The purpose of this paper is twofold. First, we outline four levels of research: metalevel research, basic research, applied research, and postintervention research. Ultimately, ISS research should lead to long-term research programs aimed at improving intervention effectiveness, which (for instance) happens through effective reporting of intervention/treatment effect rates in ISS research. Second, we highlight several unaddressed issues in ISS at each level, which can lead to new breakthroughs in ISS, including improved intervention effectiveness.

2 The "Evolution" of ISS Research

This section provides a short history of ISS research. First, in Section 2.1, we describe how the roots of ISS research stem from the birthplace of ISS management research and practice, where the focus was on outlining practical problems and solutions to them. We suggest in Section 2.2 that actual ISS research started in the 1980s and was strongly influenced by Keen's (1980) view of scientific research, which emphasized showing that reference theories taken from other disciplines are, for example, statistically supported. Later, the required contributions began to gradually shift from "new reference theory" in ISS to adding IT artifacts to reference theories—or contextualizing reference theories—as well as showing that added IT artifacts, or "contextualized theories," are empirically (often statistically) supported. We then outline several side effects resulting from this development.

2.1 The Roots of ISS Management: Describing the Problems and Proposing Solutions

ISS management research emerged in the 1970s to solve problems and improve processes in practice. For example, Donn B. Parker's (1976) work on the human aspects of computer crimes is one of the first pioneering works in this area, and Parker's definition of computer abuse continues to influence contemporary ISS research. Schweitzer's book on ISS management (1981) is an example of a pioneering work that has been followed by hundreds of others on ISS management to date. These early works were largely based on the authors' personal experiences and offered both descriptions of practice and guidance for future practice. They were case-based experience reports and recommendations.

Another example of practical problem-solving can be found in ISS checklists. Several such checklists have been produced since the 1970s (Baskerville, 1992; Siponen, 2005a,b). Since the 1990s, ISS checklists have been replaced by ISS management and maturity standards (e.g., Siponen & Willison, 2009). One of the more notable standards for ISS management is BS 7799, from the British Standards Institution, which was later developed as an ISO standard for ISS management known as ISO/IEC 17799 and later as ISO/IEC 27002. An important facet of these standards involves problems and solutions. The checklists and standards are intended to capture best practices—that is, the best solutions to key ISS management problems.

Along with the development of ISS standards and books came the establishment of conferences and journals on ISS management. In 1984, the International Federation for Information Processing (IFIP) established an ISS working group called Technical Committee 11, better known as TC11 or IFIP SEC. Since 1986, TC11 has been organizing ISS conferences. The TC11 conference is a multidisciplinary ISS conference that includes research articles on ISS management. TC11 has 14 working groups (WGs) that organize working conferences, many of which concern ISS research topics. The Roode ISS workshop (WG 11.13) is one working conference under TC11. The official journal of TC11 is *Computers & Security*, which was established in 1982 and publishes both ISS research and practical views from differing perspectives, including both computer science and ISS. Another notable journal is *Information Management and Computer Security*.

2.2 Early Information Systems Security Research in the 1980s and Keen's Influence

To understand ISS research, we need to understand the ISS environment in the 1980s. At the first International Conference on Information Systems (ICIS), Keen (1980) stressed the need for "theory" and "the dependent variable" so that ISS would not just be a theme but a "clearly defined discipline." Keen's call for theories was estimated as highly influential (Benbasat & Weber, 1996).

While previous research (and practice) in ISS management focused on describing problems and solutions, Keen's (1980) conceptualization of scientific research focused on reference theory and the dependent variable. According to Keen's scientific view, reference theories were used to explain ISS problems, so that each problem became the dependent variable. In turn, solutions could be seen as the independent variables. Research that purely described ISS problems or proposed solutions, but did not have (1) a theory, and (2) a dependent variable did not fit into Keen's (1980) view of what is scientific.

Detmar Straub's works (e.g., Straub, 1989, 1990) met Keen's standards for a "scientific base" for management information systems. Straub had reference theory (deterrence theory), yet computer abuse was the dependent variable. Straub's work then provided a model example for ISS scholars. Moreover, Straub's work introduced security into premier IS journals, such as *MIS Quarterly* and *Information Systems Research*.

We see the influence of this Keenian model on ISS research today. However, generally speaking, the idea of practical problem-solving or understanding ISS issues has persisted in contemporary ISS research since the 1970s. This is visible in the introduction sections of ISS research papers, in which the research is typically motivated by solving practical problems. Table 1 illustrates two examples (for more examples, please see the Appendix).

Table 1. Illustrations of the Practical Problem-Solving Motivations in IS Security Research

"IT security could be enhanced by using multiple methods to authenticate users, such as combining 'something you know' (e.g., a password) with 'something you have' (e.g., a smartcard or token) and 'something you are' (e.g., a biometric characteristic). Although the use of biometrics and smartcards is growing, passwords are still the most common, and sometimes the only authentication mechanism used by many organizations (Whitman, 2003). Therefore, it is important to find ways to improve password effectiveness." (Keith, Shao, & Steinbart, 2009, opening lines of introduction)	"One of the greatest concerns of IS security managers is the threat of an organizational insider. Numerous industry studies and surveys of CIOs indicate that IS security continues to be one of the top managerial concerns (Brenner, 2009; CSI, 2011; Deloitte, 2010; Ernst & Young, 2009; PwC, 2008, 2010a, 2010b)." (Willison & Warkentin, 2013, p. 1, opening lines of introduction)

As Table 1 demonstrates, it is prevalent (if not a standard practice) to motivate ISS studies with a problem in practice. Therefore, the starting point of ISS research is the practical motivation of solving problems in practice. This important assumption means that there is a relevant contribution to explicit practical problems that motivates ISS research. Philosophically, a practical motivation—a problem in practice—is the key epistemic goal of ISS research, rather than seeking truth or new knowledge for its own sake. Thus, ISS research generally originates from a *clinical* problem (or at least the papers are often motivated in that way).

Next, we describe the current state of ISS research.

2.3 Current ISS Research: New Constructs and New Relationships as Required Theory Contributions

In the past, the Keenian-inspired approach, by and large, focused on finding a reference theory (from other disciplines) that was new to ISS. To provide a simplified example of this view, theory elements (constructs) and their relationships were presented as hypotheses in which independent variables (IVs) explained (or predicted) a dependent variable (DV). This picture, therefore, required new relationships (between IVs, or between IVs and DV) and/or new elements (e.g., constructs, often modeled as IVs). In such Keenian-inspired views of science, a premium was placed on demonstrating that certain hypotheses, based on theories or previous literature, were statistically significant in a survey, archive, scenario, or some other data. In other words, new elements and/or relationships were required as a new theory contribution. Roughly speaking, the formula has been as follows:

1) Identify an ISS problem.
2) Propose a new theory/hypotheses or new constructs.
3) Show with a study that the new theory or its constructs are empirically supported.

Putting a premium on a new theory or new constructs and seeking or determining empirical support led to a situation in which ISS research was taking place in what Laudan (1978, p. 71) called a "competitive vacuum." In other words, theories (and hypotheses) were tested against some "crucial" tests showing whether the hypotheses were supported. This means that the theory's acceptance was not based on a competitive setting, featuring a "horse race" between two or more competing theories or approaches (Moody, Siponen, & Pahnila, 2018). Typically, in current ISS research, the theories, models, or hypotheses are not compared with best practices or the closest competitors. That is, current ISS research is not asking: "How can I show that my findings can outperform current best practices in solving the problem?" or "Can my approach outperform the best competitors in solving the problem?"

As a result, ISS research can show that a theory-based hypothesis (e.g., a hypothesis built upon established theories) meets some "crucial" test, but ISS research is not designed to show that the studies can beat best practices. Moreover, little is known about how any ISS study, model, or theory can be demonstrated as being better than its competitors for solving an important problem.

Generally speaking, a similar Keenian ideology also seems to hold for the few qualitative ISS papers in our top journals. Puhakainen and Siponen (2010), for example, were motivated to conduct their study due to a lack of theory-based research.

Since the introduction of information technology (IT) artifacts and theory contextualizations (Hong et al., 2014), there has been a demand to require IT artifacts or contextualizations in ISS reference theory. However, demand for IT artifacts and theory contextualizations may not have radically changed Keen's classical view of "what is scientific." An IT artifact is added to a (reference) theory, or a reference theory is contextualized as follows:

1) Introducing new elements (e.g., constructs) and/or new relationships through contextualizing a theory, or adding an IT artifact to the theory/model.
2) Demonstrating that the hypotheses (or propositions) are statistically supported (in quantitative studies) or empirically supported (in qualitative studies).

In other words, the key is showing that the IT artifact or contextualization is empirically supported—that is, that it either passes some "crucial" statistical tests (in the case of quantitative studies) or is supported by empirical material (in the case of qualitative studies). Again, as with Keen's original approach, the contextualized theories or IT-artifact-enriched theories are mainly done in a "competitive vacuum" (Laudan, 1978, p. 71). As a result, there is little demand to show how the IT artifact or contextualization adds value in beating the best practice. Furthermore, there is no demand to show that an IT artifact or contextualization of a theory solves the problem more effectively than its closest competitors. Authors may not even want to examine such questions, because they may not lead to publication in journals due to their lack of new theory contributions.

The Keenian model shifted the emphasis from problems and solutions to showing that the theory-based explanations are "true," or empirically supported. That is to say, theory-based IVs can explain (or predict) the DV, for instance. There is nothing wrong with proposing new explanations (in different forms, such as a theory or constructs, etc.). However, they should not be regarded as the final outcome of ISS research. Rather, they should be viewed as instrumental. This Keenian model and subsequent developments (e.g., IT artifacts and contextualizations) did not emphasize application effectiveness, let alone demonstrate it in a way that can be compared with best practices, or state-of-the-art research.

2.4 Some Outcomes of the Current ISS Research

As a result, practitioners seeking to enlist evidence-based practices from our most prestigious ISS journals will mainly find sets of constructs, reference theories, contextualized theories, or IT artifact-enriched models that have found empirical support. Alas, this does not indicate the best approach to practitioners or highlight which of these empirically tested theories or constructs are the most effective for solving ISS problems. More importantly, it does not clarify whether the new theories are any better than best practices or practitioners' own practices.

The aforementioned situation in ISS research is perhaps one important reason why we have not been able to lead practice. This result means that practitioners may easily turn to experience-based reports when seeking to improve their information security management. Another possible consequence is that ISS scholars may miss direct company funding. If the outcome involves the addition of a new IT artifact, the contextualization of a theory, or a new theory, then what company would want to fund this outcome? In contrast, if the outcome is “we can demonstrate to you the best approach to improve users’ password behavior,” then the funding possibilities might be improved.

There is nothing wrong with such practitioners’ thinking. Drug companies also may not want to fund a new theory for the sake of having a new theory. What drug company would want to fund the “contextualization of theories of biology or biochemistry”? Compare this with a project aimed at demonstrating that a new treatment for pancreatic cancer can offer better results than any existing treatments.

There is perhaps a more significant outcome than lack of funding—that is, lack of collaboration with practitioners, who represent huge resources for ISS research. However, it is difficult to imagine any less-attractive research outcome for companies than “establishing new statistically significant relationships, based on theory-based hypotheses.” In the IS literature, the lack of practitioners’ interest in scholarly research is justified with claims that practitioners are afraid of negative publicity (e.g., Crossler et al., 2013). These claims demand closer examination. In the ISS management literature, there is an appreciable number of research articles reporting research that was executed in company settings in different countries, including (but not limited to) the United States, Finland, the United Kingdom, and South Africa. For example, the journals *Computers & Security* and *Information Management & Computer Security* contain numerous empirical papers done in corporate or other organizational settings. Indeed, such articles also appear in the best IS journals. Examples in *MIS Quarterly* include action research papers (Puhakainen & Siponen, 2010; Straub & Welke 1998) and a field experiment (Johnston, Warkentin, & Siponen, 2015). The *Journal of the Association for Information Systems* (*JAIS*) has also published ISS research carried out in a company setting (Siponen, Baskerville, & Heikka, 2006). The concern about bad publicity is understandable if the companies are asked to report their specific ISS breaches or if the study describes specific cases of incompetent ISS practices. However, bad publicity seems to be an irrelevant concern in survey or experimental research settings. For example, suppose researchers test protection motivation theory (PMT) in a company using a survey or experimental approach. If the results reveal that only one PMT construct explains security behavior, what bad publicity could possibly result for a company whose identity is not revealed? If there were any negative publicity at stake in such a case, it would be negative publicity for PMT rather than the company.

We argue that the lack of interest in practice could be partly improved by adding a layer of research that focuses on problem-solving effectiveness.

Another related outcome of the current situation is that ISS research does not seem to lead practice. For example, it appears that even the best ISS works exert little influence on ISS management standards. Information security journals, such as *Computers & Security* and *Information Management & Computer Security*, contain articles that often recommend that practitioners follow ISS management standards (e.g., von Solms, 1998, 1999; von Solms & von Solms, 2004). However, such standards fail to cite any ISS journal articles (Siponen & Willison, 2009). Neither these articles nor these standards advise practitioners on how to follow findings reported in even the best IS journals.

As a further example, consider the extent to which state-of-the-art, cutting-edge ISS research, such as that published in top IS journals, influences the content of ISS business seminars. For example, oncology conferences (for clinical practitioners) are replete with university-sourced, science-based presentations. By comparison, business seminars on ISS management, generally speaking, feature far fewer ISS research presentations. Thus, it is difficult to claim that top IS journals are shaping or leading practice.

Arguably, there are numerous reasons why ISS research does not lead practice, including long publication life cycles compared with natural sciences, long articles that focus heavily on theory and methods, the use of jargon related to theory and methods, and lack of commonly required IT education (cf., certified medical doctors). Next, we discuss an important point in terms of leading practice.

2.5 ISS Research: Toward Leading Practice

Cancer research, rather than non-research-based practice, arguably leads oncological practice. Our interest is in determining what it means for something to lead to practice. We suggest that an important indication of research-led practice is denoted when *the interventions based on academic research offer significantly better effect rates than any intuitive or experience-based approach that is not science based*. In other words, the interventions based on academic research must outperform the best industry practices. The more that such problem treatments are based on ISS research and offer significantly and demonstrably better effects, the more ISS research will be capable of leading practice. The more that such effect rates outperform intuitive or experience-based practitioner solutions, the more reasons there would be for practice to follow research. International standards and practice conferences could grow increasingly dependent on the great results of ISS research if they were to clearly outperform the best previous practices. Certifications, such as the CISSP, also could draw from the essential content of research. It also could increase the demand for ISS scholars to appear at select business seminars, where their research provides both the know-what and know-how that are essential to practice.

Research leading to practice is a solid aim, both ethically and professionally. Ethically, it increases the contribution of university research in a socially important problem area: ISS. Professionally, it sets the stage for ISS practice to become more soundly evidence-based. For evidence-based management, practice needs both evidence from the problem setting (the symptoms) and scientific evidence indicating the appropriate treatment (the cure).

Aiming to expand ISS research to include relevance-by-treatment does not eclipse or suppress existing ISS research. Instead, intervention-oriented research can be built on previous work.

3 Four Levels of Research

Figure 1 illustrates how the aims of the ISS research discipline must expand. Improved intervention/treatment effects are the ultimate goal of ISS research. Individual studies fall typically into one or more of these categories. Levels can inform each other and can, of course, overlap. It has been fashionable to associate IS approaches to big philosophical *-isms*, such as logical positivism (see Siponen & Tsohou, 2018), logical empiricism (e.g., Hempel, Reichenbach), critical rationalism (Popper), or critical realism (e.g., Niiniluoto). Our approach is not influenced by such professional (school) philosophers but by the philosophy of cancer research (Klaavuniemi & Siponen, 2018). Our proposal also has some similarities and differences with evidence-based management (Pfeffer & Sutton, 2006; Rousseau, 2006). A discussion of the similarities and differences could constitute its own article.

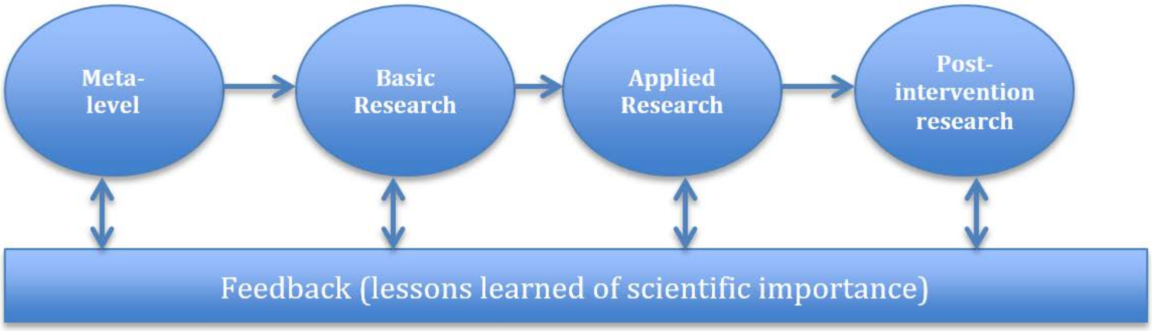
Meta-level
Basic Research
Applied Research
Post-intervention research
Feedback (lessons learned of scientific importance)

Figure 1. Illustrates the Idea of a Research Discipline Transformation using a Simplified View of a Stepwise Approach

The figure illustrates how research produces disciplinary knowledge at four progressive levels. The following description of the four levels is a first approximation. The metalevel regards fundamental issues, such as concepts, methodology, and scope. Basic research explains phenomena—that is, the know-what knowledge that engages relevance-by-description. Applied research engages relevance-by-treatment or the know-how knowledge that tackles problems. Postintervention research explains why treatments (did not) produce effects. Table 2 provides examples of these levels. In the following sections, we describe each level in more detail.

Table 2. Definitions of Variables

Example of research levels	Example description of key issues	Examples of estimating contributions
1) Metalevel	Definitions that guide research on ISS phenomena, important problems, the differences between ISS phenomena, and defining ISS.	Are the existing definitions good enough to guide research? What does the phenomenon mean? How is the phenomenon different from other, related phenomena?
2) Basic research: Theory development and revision	Providing explanations for phenomena.	How is the explanation new in clarifying specific ISS phenomena? Are the explanations for specific ISS phenomena more accurate than rivaling explanations?
3) Applied research: Interventions to test the effect rate	Demonstrating the effect (rate) for intervention/treatment for X.	How does the intervention based on a new approach provide better effect rates than competing approaches? Does the intervention based on the new approach have another positive or negative characteristic that competing approaches do not have?
4) Postintervention research	Explaining intervention results, effect rate, complications, or long-term effects.	Challenging existing studies. What is the long term effect of an ISS approach?

3.1 Metalevel

Metalevel issues refer to fundamental issues in the research area and typically are conceptual-theoretical. They can be of utmost importance because they may set or change the direction for future research at the other levels. We have seminal examples of work at this level. Baskerville's idea of development duality (Baskerville, 1986, 1988, 1992) claimed that IS or software development and security development often represent two separate streams of development (and research). This duality results in conflicts between systems' normal requirements and security requirements. Resolving these later in development, or when the software is already finished is difficult, costly, and may cause new problems. Baskerville's idea of development duality is, in the opinion of this paper's first author, a great example of how ISS research could lead practice and change secure systems development in the long run. For example, there are many software security patches and frequent new releases. Is this situation partly due to the inadequate consideration of information security during the initial software development?

3.2 Basic Research

In the ISS context, basic research, for instance, seeks fundamental explanations for specific ISS phenomena. In our model, basic research is carried out in artificial conditions. In this case, they are self-report surveys, scenario-based research, laboratory experiments, and the like. Basic research is typically oriented toward new idea development or theory development. When it comes to theory testing, it entails finding the limitations and conditions that hold (or do not hold) concerning an already developed theory or idea.

It is also important to note that theory evaluation is not a black-and-white, yes-or-no result. Even the best theories in science can draw both supportive and nonsupportive evidence (Laudan, 1978). It is important to put forth scholarly efforts to identify the exact limits of a theory or an approach. Knowing the conditions or situations under which the theory/approach does not hold is an important source of inspiration for future research. Reporting such information can help scholars extend or revise extant theories/approaches or develop new, rival explanations. Finding the limits and situations in which the theory may be unable to explain phenomena is highly important in ISS. Such limiting conditions are important because ISS is regarded as a weak-link phenomenon (Willison & Warkentin, 2013). The weak link, or breaking point, for information security can be a certain situation or those people who ignore all ISS messages and do not participate in surveys. Given this, there is a need to know in which contexts and in which situations our models/theories fail to provide explanations or predictions.

Basic research is important for many reasons. If we lack new ideas (at the level of basic research) or we cannot identify new problems using existing approaches at the level of basic research, we risk having far fewer ideas to cultivate in order to further improve the intervention effect rate and, therefore, ISS practice. Moreover, besides new explanations, we need a much more detailed understanding of what these explanations mean in different settings and contexts. We also need to know where they work and where they do not work. We call all of this *basic research*, much of which must be done in nonfield settings (why it is called *basic research*). In theory, we could do basic research in practice (e.g., at companies), but in practice, it would be difficult to do such studies in company settings. For example, it is difficult to access "real" settings in companies in which one can vary, say, subjective norms or sanctions for employees. For company-level (field) testing, one suggestion would be to use approaches that are already widely examined in basic research. However, ISS approaches are not yet widely examined at all. In particular, their limits and concrete instantiations (e.g., what exactly is an effective subjective norm or sanction) are not studied widely.

3.3 Applied Research

A major goal of applied research is to move basic research to applicable results in practice. However, applied research does not necessarily need to be based on basic research. In biology and biochemistry, for example, it is widely known that many of the results of basic research do not survive and move up to the intervention research level or reach the stage of application or drug development. It is often the case that basic research findings are too abstract or lack sufficient specifics to be applied as such in practice. One important issue in the applied research is the effect rate for the intervention/treatment. This rate enables comparisons between the effect rates for an intervention based on a new approach with those of competing approaches. Indeed, an intervention based on a new approach may have other positive or negative characteristics that competing approaches do not have. Research methods used at this stage include (but are not limited to) action research, case studies, design science research, and field experiments.

3.4 Postintervention Research

Postintervention research takes place after the intervention has happened at the applied research level. Postintervention research is needed to learn from interventions. For example, in medicine, drug complications in hospitals are reported. Several scientific breakthroughs have resulted from postintervention research. Studying recovery rates after surgeries or cancer treatments in medicine is also a good example of postintervention research. Exemplary research issues examined through postintervention research include explaining the unexpected results of an intervention. Another highly important issue is explaining an effect rate that was found to be far less than what it was assumed to be. Other issues include the complications of an intervention (if any) and the long-term effects of an intervention.

3.5 ISS Examples

3.5.1 Metalevel Examples

The metalevel encompasses fundamental issues, such as concepts, methodology, and scope. One of the earliest definitions in the area of insecure behaviors is Parker's (1976) definition of the term *computer abuse*. Later, Straub (1990) introduced it to ISS, and this paper's first author might be to blame for introducing the terms *information security policy violations* and *employees' noncompliance with information security procedures* (Siponen & Vance, 2014).

Parker's definition of computer abuse is as follows: "Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain" (p. 12). Later, possibly motivated by Parker, this term was defined in the ISS field as follows: "The unauthorized and deliberate misuse of assets of the local organizational information system by individuals" (Straub, 1990 p. 257; see also Harrington, 1996; D'Arcy, Hovav, & Galletta, 2009).

One important issue that these definitions fail to capture is whether various ISS behaviors are different from each other. There is no doubt that many, if not all, of the behaviors studied under *computer abuse* or *employees' compliance with IS security policies* are motivated by ISS concerns. For example, topics such as selecting an easy-to-guess password or putting confidential material without encryption onto a USB stick may result in ISS concerns. Accordingly, both actions may have ISS implications. Thus, both actions can be regarded as insecure, which perhaps results from their potential risk.

Indeed, it seems to us that the insecure or risky nature of different insecure ISS actions—from not locking a computer, to selecting an easy-to-guess password, to sending confidential information without encryption in e-mails, etc.—has been the driving motivation for ISS research. At the same time, little (if any) consideration has been devoted to whether all insecure behaviors are ultimately of the same nature. This has been made apparent in ISS research in two ways:

1. Our definitions, whether concerning computer abuse or ISS policy violations, are generic in the sense that they do not distinguish between different types of insecure behaviors.
2. In general, the models used to explain insecure behaviors are generic to different ISS behaviors.

Let us begin with the definitions. *Computer abuse* refers to "the unauthorized and deliberate misuse of assets" (Straub, 1990, p. 257). The concern is unauthorized and deliberate misuse. The existing definitions do not distinguish between different insecure behaviors and do not point scholars in the direction of examining different insecure behaviors. Quite the opposite—scholars may interpret the definition of *computer abuse* in the sense that anything that constitutes "unauthorized and deliberate misuse of assets" in ISS is computer abuse. This can explain why employees' non-work-related use of the Internet is sometimes regarded as computer abuse.

Similarly, the definition of *ISS policy violations* (or employees' noncompliance with ISS policies) refers to policy violations (e.g., Siponen & Vance, 2010) as if all policy violations represented one kind of infraction. In other words, the definition implies that all ISS policy violations are the same.

Such generic definitions prompt us to reconsider generic models. The generic nature of our definitions for computer abuse, policy violations, and employees' compliance overlooks the individual nature of these behaviors. This generic-ness explains why previous ISS behavior research focused on identifying users' reasons for exhibiting insecure behaviors—that is, because these reasons are (believed to be) generalizable to all kinds of ISS behaviors. As a result, previous research put a premium on models in which the same reasons, such as fear of threat or sanctions, explain users' ISS behavior across all insecure behaviors (e.g., selecting a weak password, not locking a computer, etc.). Generic measures represent the most common method for measuring insecure behaviors in previous research (Siponen & Vance, 2014). These include evaluating responses to prompts, such as "I comply with the information security policies of my organization" (ibid). They are generic because they do not point to (or measure) a specific insecure behavior.

There is nothing wrong with finding generic reasons that are indeed common to different ISS behaviors. However, it is important to understand how different ISS misbehaviors (e.g., not locking one's computer and writing passwords down) may have similar ISS implications. These actions are not necessarily motivated by the same kinds of reasons. We should not confuse the *information security implications* of an action with the *reasons* why the action was or was not undertaken. Putting this argument in the context of computer abuse or ISS policy violations, the fact that something is a policy violation or computer abuse (or "unauthorized deliberate misuse") may not mean that all policy violations or computer abuses are motivated by the same kinds of reasons. Rape, murder, and speeding are all violations of the law, but the fact that they are against the law does not mean that these three actions all have the same motivations. The possibility that different ISS behaviors are motivated by different factors is not present in the existing definitions above.

It could be that these insecure behaviors have little in common, aside from being insecure behaviors. Rape and speeding are both violations of the law, but their underlying motivations are generally very different. Let us illustrate this with a deterrence theory example. Deterrence theory is currently one of the leading theories in ISS. It describes sanctions for insecure behaviors (Willison & Warkentin, 2013). Deterrence theory may apply to criminal behavior, but it does not make sense for all insecure behaviors. For instance, weak password selection can occur because some users cannot memorize a password. Sanctions can hardly improve human memory. Adopting the same method in practice can also limit impact. Sanctions are not necessarily realistic for resolving all types of insecure behaviors.

There is nothing wrong with examining individual reasons or motivations in terms of DVs or IVs that are common for different ISS behaviors. However, there is also a need to understand how these reasons or motivations differ for various ISS behaviors. Current definitions hint at generic reasons, but they necessitate definitions of different ISS behaviors.

3.5.2 Basic Research Examples

Basic research, for example, involves explaining phenomena regarding theory development and discovering theories that explain (or fail to explain) a phenomenon. Often, IS research consists of testing a reference theory on the basis of a one-shot survey that may lack all of the important situational conditions. Typical research methods at this level include surveys, experiments, interviews, and case studies.

Reference theories used in ISS should receive critical attention in basic research. Kuhn (1977) noted that in science, concepts with the same name can mean very different things, even within one discipline. For ISS, one important question is whether the fundamental concepts in the reference theory have the same meaning in ISS phenomena as they have in the originating phenomena of the theory. Let us use a *fear of threat* example from PMT. PMT is based on fear of threat in a health behavior, such as fear of dying or fear of getting cancer from smoking (Rogers, 1975). ISS actions or behaviors, such as weak password selection, may be linked to a threat or lack of a threat. In PMT, ISS research must clarify descriptively whether the kind of fear over the theft of one's password is the same kind of fear to which PMT originally referred. For instance, can we equate fear of dying from tobacco use with the fear of lost privacy from a comprised e-mail? Both events pose threats, but the fear may be different. Indeed, the latter may not even theoretically satisfy the meaning of fear in the sense of PMT. It may just be threat avoidance that does not involve fear, such as in the threat avoidance model proposed by Liang and Xue (2010), which does not include fear at all.

Similar questions confront any reference theories. For example, neutralization techniques also face such questions (Siponen & Vance, 2010). Basic ISS research attacks and examines such fundamental issues.

Metalevel research occurs when researchers examine these questions conceptually (with or without reference to published empirical evidence). Basic research arises when researchers examine these questions empirically. Where we may lack information regarding specific cases or situations in which the theory does or does not hold, it becomes necessary to test our theories using the same methods in different contexts and situations to determine the exact boundaries and applicability.

3.5.3 Applied Research Examples

Applied research engages relevance-by-treatment—that is, know-how interventions that produce effects on problems. For ISS behavioral research, *applied intervention research* is research that, for example, changes users' insecure behavior into secure behavior. Applied research can be proactive. For instance, we need research on interventions that overcome people's inhibitions toward using protective IT security technology (Dinev & Hu, 2007).

Most important is the need to report intervention effect rates. For example, if a contextualized PMT intervention improves computer-locking rates by 15%, it provides a measurable target which research can use to potentially improve the effect rate. Thus, if a treatment based on PMT version 1 yields a 15% effect rate (improved behavior), and a second treatment based on PMT version 2 yields a 25% effect rate, then the better effect rate is clarified and motivates improvement research. The metaresearch issue of who has a pure, original, or orthodox application of PMT (Boss et al., 2015) is irrelevant in practice, unless the distinction is visible in the effect rate.

This comparability provides the power in practice that arises from relevance-by-treatment. We might even learn that a combination of theories 1 and 2 continues to provide better effect rates than either theory 1 or theory 2 alone. In such circumstances, it is irrelevant in practice to criticize an article lacking an overarching theory just because there is a need to have one for good form. Such overarching theory can be deferred to subsequent postintervention research intended to descriptively investigate why the applied results find that the combination of theories 1 and 2 yields better effect rates. Such further postintervention research achieves relevance-by-description in finding a new overarching theory.

Examples of such applied research include Puhakainen and Siponen (2010), Warkentin and Johnston (2010), and Johnston et al. (2015). Siponen and Puhkainen reported multicycle action research interventions that improved employees' e-mail encryption practices at a small company, while Warkentin and Johnston and Johnston et al. described online campaigns using fear appeals to scare users into better password security, avoiding insecure use of USBs, and locking their computers. However, we could not find an ISS study that explicitly reported an intervention effect rate. If researchers hope that ISS research can reach a point where it actually contributes to solving practical problems, they must also direct their efforts at intervention research that has the improvement of intervention effect as a key goal. For example, an experimental study on fear-appeal messages regarding password changes could report what percentage of users changed their passwords due to the fear-appeal message.

Evidence-based management (e.g., Rousseau, 2006), which is influenced by (beliefs about) evidence-based medicine, suggests that evidence-based management (and medicine) is characterized by straightforward causal (effect) relationships. However, such causality is highly questionable in the context of medical research and psychology (Thagard, 1998). Therefore, it is important to highlight that the intervention effect rate is not fixed once and for all, but is dynamic and cancer-specific, even in cancer research. The intervention effect can also be context-specific and situational. For example, diffuse large B-cell lymphoma (DLBCL) is one type of cancer (Klaavuniemi & Siponen, 2018). For instance, in DLBCL, at the 2-year follow-up point, 70% of patients treated with rituximab and chemotherapy were alive, compared to 57% who received only chemotherapy (ibid; Coiffier et al., 2010). The intervention effect rate of chemotherapy to DLBCL can be said to be 57%, while the intervention effect rate of rituximab and chemotherapy is 70%.

The intervention effect rate can be seen as a statistical average. In practice, this means that the effect of chemotherapy (treatments) varies from patient to patient (Klaavuniemi & Siponen, 2018). One dies before the two-year follow-up, another stays alive up to that point (ibid) or even longer; for a third patient, the chemotherapy can have lethal side effects (ibid). The intervention effect rate studies also may vary from one study to the next, for example, because cancers hardly follow laws (Thagard, 1998; Klaavuniemi & Siponen, 2018).

Without going into detail about the philosophy of science, we also assume that the intervention effect rate is highly dynamic, contextual, and situational in IS, for example, due to human intentionality. It is expected that different ISS approaches have different intervention track records in different settings. Furthermore, since we assume that there are no laws determining human behavior, we expect the possibility of inconsistent results. Let us presume that Jack receives a fear-appeal message (in terms of PMT) from his organization. The message asks that he change his work password as soon as possible and make it as unique as possible (not generic to different accounts). Accordingly, Jack changes his password and makes it unique. However, later, Jack continues to use generic or reused passwords (that are the same or very similar for different accounts). Later, Jack receives the same message again, which asks that he change his password as soon as possible and make it unique (not generic to different accounts). However, he does not comply, since he thinks that nothing has happened to him (he did not perceive any ISS problems), even though he reused his password across different accounts (generic password). PMT (and many well-known theories) cannot fully explain such dynamics. This is one reason why we assume that inconsistent results are common.

Next, we describe briefly what this means practically with respect to the intervention effect. We hesitate to suggest any number of minimum or maximum tests. Rather, we use the concept of an *intervention-effect track record*, which contains evidence for each empirical test with respect to each approach. As a simplified example, the track record of personalized fear appeals could be 25% for changing a password for the first time, or it could range from 15% to 35% in most studies. For repeated fear appeals to the same person, the results could change. However, for the use of e-mail encryption, the results could be different. Moreover, for illustration purposes, the intervention-effect track record could be understood as stages of development. For example, although cancers do not follow stages, cancer treatments and health behaviors are sometimes conceptualized as occurring in stages. By adopting such an approach to ISS, stages could be developed for the continued use of, for example, antimalware software.

The point is to show that the intervention effect rate could be linked to the type of ISS violation (e.g., not encrypting e-mails versus passwords reuse), according to each "stage," specific contexts or situations, and according to many other dimensions that we have not even defined yet. However, we would not seek to define a priori to which aspects the intervention-effect track record are related, because that is also an empirical question.

Finally, long-term effectiveness should be studied. Let us consider a comparison of two theories or approaches, called T1 and T2. T1 achieves 40% effectiveness right after the intervention, while T2 achieves 28%. However, after 6 months, T2 achieves 25%, while T1 achieves 5%. This exemplifies a study on long-term effects. Such studies published in ISS are rare. One reason is that such studies may lack new theory contributions in the eyes of reviewers, because no new constructs are introduced. However, being aware of the long-term effectiveness could be much more valuable than a new theory contribution (e.g., introduction of new constructs).

3.5.4 Postintervention Research Examples

Postintervention research explains why treatments produce, or do not produce, effects. This level of research provides necessary feedback for further theory development. Such theories will explain in detail why ISS interventions succeed or fail in certain situations, and why there are certain effect rates (e.g., why only 25% changed their password in the case of password training or campaigning, and why 75% did not). An example of postintervention research is the use of a qualitative study to obtain "additional insights on the findings from a quantitative study" (Venkatesh, Brown, & Bala, 2013 p. 6; Venkatesh, Brown, & Sullivan, 2016). Of course, postintervention research does not have to employ interviews. Any methods that fit the purpose can be used.

In ISS, postintervention research is largely missing, with the exception of the aforementioned example of an action research setting in which the second cycle is based on the analysis of improving the first cycle (i.e., Puhakainen & Siponen, 2010). Puhakainen and Siponen (2010) did their intervention in a company where sales teams were sending e-mails without encryption—as was the rest of management (including the CEO). This reckless, top-down attitude toward appropriate ISS behavior was a key aspect of the problem. They implemented a face-to-face training program to increase compliance with the company's e-mail policy (Puhakainen & Siponen, 2010). Then they analyzed the results of the intervention using data from several interviews and observations by the researchers and the security manager. The results (postintervention scrutiny) suggested that while the intervention made the sales team encrypt confidential e-mails, management remained extremely passive regarding security (Puhakainen & Siponen, 2010). The second intervention was aimed at improving management's attitude and actions. The interviews and observations after the intervention (postintervention research) suggested that management's ISS behavior had improved.

4 Applicability of Our Ideas beyond IS Security and Further Developments

We believe that that our ideas may fit with many other areas of IS, including (but not limited to) IT use and design science. Let us consider a well-known example in IT use—namely, ease of use (Venkatesh, Thong, & Xu, 2016). For example, ease of use could be further associated with concrete system features and then examined to determine to what extent improving these concrete system features actually improves IT use. Then the intervention effect rate could be the rate of IT use, for example. Then different approaches could be compared to determine the extent to which they can improve the rate of system use through improving the ease of use of system features.

The idea we have proposed could also be used in design science. For example, let us imagine software testing in the area of software development. If the aim of the software testing is to reduce errors, then one important effect rate relates to the question of which method has the best track record of reducing coding errors. The aims must be articulated before we can nominate candidates for the intervention effect rate. In ISP violations, which we discussed in the paper, there seems to be an agreement that a key outcome is improved ISS behavior. In this case, an important intervention effect rate question would be the following: "Which approach provides the best track record of improving users' behavior?" For example, if an intervention based on PMT provides a 20-25% change rate for, say, locking a computer in different settings, then can the contextualized PMT or some other approach achieve a higher change rate? We would need dedicated papers to outline how our proposal can be applied in other areas of IS. Therefore, we leave this to future research.

While our approach may be not applicable to all research, we believe that it applies to what Astley and Zammuto (1992) called symbolic utilization, which entails the use of models, metaphors, and theories for justifying actions, ideas, or decisions (p. 452). For Astley and Zammuto, such symbolic information is purposely abstract and vague to allow for multiple meanings (p. 457). Our suggestion is to examine these issues using the intervention effect. For example, if there is a claim that abstract and vague concept X is effective in justifying something occurring in organizations, then we could actually study its intervention effect. In fact, we could examine Astley and Zammuto's whole idea by examining whether such symbolic information is effective for justifying actions, decisions, or ideas, and what its "side effects" are.

We also want to emphasize that there may not be one ultimate yardstick for the intervention effect rate. In software testing, it could be reduced coding errors, while in insider (computer) crime, it could be the number of solved cases and improved rates of computer crime prevention. However, these are just illustrative examples. It is up to future researchers to consider what the proper measures would be for using the intervention effect rate. This should also become an active research area. What a proper measure or estimate of the intervention effect is also depends on the aim of the research. Moreover, it is important to note that the intervention effect is not necessarily only one thing. For example, cancer treatments are valued according to numerous indicators, such as improved life expectancy and minimization of severe side effects (Klaavuniemi & Siponen, 2018). To illustrate this in the ISS context, let us presume a considerable increase in the threat of sanctions (as an intervention) at an organization. This could improve ISS behavior, but it might also decrease work satisfaction. While individual studies could focus on one of these consequences, the research programs on sanctions should perhaps take both (and perhaps many other) indicators into account. Thus, perhaps the best research program would be the one with the best track record for improving ISS security behavior without (or with minimal) side effects. However, future research should discuss this.

Finally, many of our ideas require further development. For example, if IS research is to be practically applicable, there is a need to develop measures for practical or clinical significance, which is not the same as statistical significance (e.g., Thompson, 2002). Another important point is to examine how the evidence (e.g., intervention effect rate) should be applied in an environment where there are no natural laws and the causality is complex (Thagard, 1998) or random (Dupré & Cartwright, 1988). As mentioned in the DLBCL chemotherapy example, the research results on cancer treatments often require individual application on a per-patient level. This is also expected to be the case in IS security.

Moreover, as mentioned, empirical ISS research has focused on demonstrating that the results are statistically supported (in quantitative studies) or empirically supported (in qualitative studies). However, IS (security) research must also examine precision (Edwards & Berry, 2010). To give a simple example, painkillers are ineffective if the dosage is very low. Yet if the dosage is very high, they might kill the patient.

Moreover, for historical reasons, many theories used in IS are rather high-level and generic; hence, we lack details to apply models and theories in practice as such. For example, let us presume that a study applying the theory of planned behavior suggests that subjective norms explain ISS behavior. It is a very different thing to establish that link in a survey, for example, compared to showing how subjective norms can be transferred to practical applications. To illustrate this, we ask what "subjective norms" findings mean in practice. If the results indicate that a subjective norm is "significant," what must the practitioners do precisely? What do they need to do to increase subjective norms? Who defines the norm? How much is needed? What if there is too much emphasis on subjective norms and, as a result, providing subjective norms backfires? Current ISS research does not have answers to these questions, and the current method (propose a theory and test it, then propose another theory and test it) does not support such development in that direction. The lack of information also prevents practical applicability. Results such as "increase subjective norm" are often too vague to have applied value. As long as we cannot produce answers that offer a detailed level of explanation for an IS phenomenon, our results cannot really be used in practice.

5 Directions for Future ISS Research

We have suggested that ISS research should be seen in terms of long-term research programs, which comprise four levels: metalevel research, basic research, applied research, and postintervention research. The ultimate success of such research programs is not to be judged in terms of whether new theories and contextualized theories have been developed, or whether IT artifacts have been incorporated into the theories. Rather, the ultimate success of such research programs hinges on the question of which program can demonstrate the best track record of intervention effect rates for a given ISS problem. While we have presented our approach in the context of ISS, our approaches could be applied more widely in IS.

5.1 New Opportunities for Metalevel Research

Current definitions in ISS reflect definitions of computer abuse from the 1970s. Leading theoretical inspirations come from applying decades-old theories from economics, criminology, and health behavior to different ISS aspects. Intervention research is largely missing, not to mention long-term intervention research.

The need for definitions is an example of new research opportunities at the metalevel. These current definitions assume that "computer abuse" or "IS security policy violations" are one type of behavior (e.g., all ISS policy violations spring from the same motivations), although it could be that computer abuse or ISS policy violations involve several different types of behaviors. This offers new opportunities for future research.

Research method norms are another example of a metalevel research opportunity. Research methods should not be considered universal dogmas. Instead, they need to be considered in a case-by-case context. Equally important is understanding that research methods have different roles—not only concerning whether the research is quantitative or qualitative but also whether the research aims at new theory development, theory revision, testing, or a more specific goal. Theory contextualization is common in ISS. Such contextualization thinking should be extended to research method principles. The contextualized nature of research methods offers ISS scholars new avenues for context-specific method development.

5.2 New Opportunities in Basic Research

In many areas of ISS, theorizing has followed the form of "find a new reference theory for IS security and test it" (cf., Grover & Lyytinen, 2015). As a result, little is known about what is specific in an ISS phenomenon versus reference theories, because the research has been driven by reference theory rather than ISS phenomena. Second, little is known about which (reference) theories or approaches work better than others in solving different ISS problems, because the reference theories are often not compared against each other. Third, little is known about the limitations and inapplicability of existing approaches and theories for solving various ISS problems. These issues offer great opportunities for basic ISS research. Not only can IS scholars develop more specific theories that leverage the richness of various IS phenomena but IS scholars can consider the conditions and boundaries limiting the use of reference theories to explain various ISS phenomena. The latter requires shifting our thinking from "one test is needed to test a theory" (or "Where can I find the one setting to support the model?") to the attitude that our theories/models/approaches must be tested many times in different settings. The fact that many of these theories/models will not explain several of their predisposed situations is not a failure of science but is actually widely acknowledged in science. From Kuhn (1978) to Laudan (1962), such anomalies can inspire future research and progress. Such progress will be far more limited if it reflects the following formula: *Pick theory 1 and test it, then move to theory 2 and then test it*. While this provides a continuous stream of research, it does not move us into a position to lead and guide practice. If we instead examine the conditions (e.g., country / culture / behavior / context / situation) under which one of these theories will consistently hold (or fail to hold), then we will have made progress. The anomalies are particularly important in ISS because it is known to be a weak-link phenomenon. The anomalies and various limitations of the theories/models can also inspire further research and the development of competing theories aimed at improving some of the limitations and anomalies.

5.3 The Blue Ocean in Applied and Postintervention Research

Given the ethical gravity of our aim (that ISS research contributes to problems of insecurity in practice), contributions cannot happen if basic research is not further cultivated toward applied intervention/treatment research. We should not view the final outcome of ISS research as a new reference theory, new theory contribution, contextualized theories, or IT artifact-enriched models/theories. Rather, we should approach theories (with or without IT artifacts) as research programs that can ultimately lead researchers toward "basic research"—i.e., increasingly improved problem-solving effectiveness regarding a problem in practice. According to this view, in ISS behavior, for example, the ultimate yardstick for the success of a theory/model in the area of ISS behavior is its measurable record of showing that interventions/treatments lead to improved effect rates. In this view, ultimately, contextualized theories or IT artifact-enriched theories add value if they lead to improved intervention effect rates. By taking this relevance-by-treatment approach, ISS research can lead practice by enabling evidence-based practice. The rise of this approach will mark a milestone in which ISS interventions based on ISS research offer significantly better effect rates than any intuitive or experience-based approach adopted by practitioners.

Acknowledgments

We would like to thank Tuula Klaavuniemi, PhD, MD, for the cancer and medical-research examples and clarifications on the role of basic, applied, and postintervention cancer research, as well as the role of treatment-effect rates in oncology. Moreover, we want to thank EIC, Prof. Suprateek Sarker, Dr. Ryan Wright, Dr. Anthony Vance, Dr. Mikko Rönkkö, Dr. Arto Ojala, Dr. Wael Soliman, and Dr. Michael Cuellar for their valuable comments. We also thank reviewers for their comments concerning the paper.

References

Abbasi, A., Sarker, S., & Chiang, R. (2016). Big data research in information systems: Toward an inclusive research agenda. *Journal of the Association for Information Systems, 17*(2), i-xxxii.

Abrahamson, E. & Fairchild, G. (1999). Management fashion: Lifecycles, triggers, and collective learning processes. *Administrative Science Quarterly*, *44*(4), 708-740.

Alter, S. (2001). Recognizing the relevance of IS research and broadening the appeal and applicability of future publications. *Communications of the Association for Information Systems*, *6*(3), 13-17.

Astley, G. & Zammuto, R. (1992). Organization science, managers, and language games. *Organization Science, 3*(4), 443-460.

Baskerville, R. & Dulipovici, A. (2006). The theoretical foundations of knowledge management. *Knowledge Management Research & Practice*, *4*(2), 83-105.

Baskerville, R., & Myers, M. D. (2009). Fashion waves in information systems research and practice. *MIS Quarterly*, *33*(4), 647-662.

Baskerville, R. (1988). *Designing information systems security*. New York, NY: Wiley.

Baskerville, R. (1989). Logical controls specification: An approach to information systems security *Systems Development for Human Progress*, *25*(4), 241-255.

Baskerville, R. (1991a). Risk analysis as a source of professional knowledge. *Computer & Security*, *10*(8), 749-764.

Baskerville, R. (1991b). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, *1*(2): 121-130.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, *25*(4), 375-414.

Benbasat I. & Weber, R. (1996). Research commentary: Rethinking "diversity" in information systems research, *Information Systems Research*, *7*(4), 389-399.

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

Boss S., Galletta, D., Lowry, P., Moody, G., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly*, *39*(4), 837-864.

Coiffier, B., Lepage, E., Brière, J., Herbrecht, R., Tilly, H., Bouabdallah, R., . . . Gisselbrecht, C. (2002). CHOP chemotherapy plus rituximab compared with CHOP alone in elderly patients with diffuse large-B-cell lymphoma. *New England Journal of Medicine*, *346*(4), 235-242.

Crossler, R. & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems, 18*(7), 487-515.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(1), 90-101.

D'Arcy, J., Hovav, A., & 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.

Dupré, J. & Cartwright, N. (1988). Probability and causality: Why Hume and indeterminism don't mix. *Nous*, *22*(4), 521-536.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44.

Feyerabend, P. (1975). *Against Method: Outline of an Anarchist Theory of Knowledge*, London: New Left.

Grover, V. & Lyytinen, K. (2015). New state of play in information systems research: The push to the edges. *MIS Quarterly*, *39*(2): 271-296.

Hong W., Chan F., Thong J., Chasalow, L. & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111-136.

Johnston, A. C. & Warkentin, M. (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

Johnston, A., Warkentin M., & Siponen M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134.

Karjalainen, M. & 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): 518-555.

Keith, M., Shao, B., & Steinbart, P. (2009). A Behavioral Analysis of Passphrase Design and Effectiveness. *Journal of the Association for Information Systems, 10*(2), 63-89.

Klaavuniemi, T. & Siponen, M. (2018). *On the philosophy of intervention research: An example from cancer research*. Unpublished manuscript.

Keen, P. (1980). MIS research: Reference disciplines and a cumulative tradition. In McLean, E. R. (Ed.), *Proceedings of the first international conference on information systems* (pp. 9-18). Philadelphia, PA: ACM Press.

Keen, P. (1991). Relevance and rigor in information systems research: improving quality, confidence cohesion and impact. In H.-E. Nissen, H. Klein & R. Hirschheim (Eds.), *Information systems research: Contemporary approaches & emergent traditions* (pp. 27-49). Amsterdam: North-Holland.

Kogut, B. & Zander, U. (1997). Knowledge of the firm. Combinative capabilities, and the replication of technology. In L. Prusak (Ed.), *Knowledge in organizations* (pp. 17-35). Boston, MA: Butterworth-Heinemann.

Kuhn, T. S. (1962). *Structure of scientific revolutions*. Chicago, IL: University of Chicago Press.

Kuhn, T. S. (1977). *The essential tension: Selected studies in scientific tradition and change*. Chicago, IL: University of Chicago Press.

Laudan, L. (1978) *Progress and its problems: Towards a theory of scientific growth.* Berkeley: University of California Press

Laudan, L. (1996) *Beyond positivism and relativism: Theory, method, and evidence*, Boulder, CO: Westview.

Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Moody, G., Siponen, M., & Pahnila, S. (2018) Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42*(1), 285-311.

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

Pfeffer J. & Sutton, R. (2006). Evidence-based management. *Harvard Business Review*, 84(1), 1-12.

Ponemon Institute. (2016*). 2016 cost of data breach study: Global analysis.* Traverse City, MI: Ponemon Institute.

Privacy Rights Clearinghouse. (2016). Chronology of data breaches. Retrieved from https://www.privacyrights.org/data-breaches.

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

PwC. (2016). Turnaround and transformation in cybersecurity. Retrieved from https://www.pwc.com/sg/en/publications/global-state-of-information-security-survey.html

Robey, D. & Markus, M. L. (1998). Beyond rigor and relevance: Producing consumable research about information systems. *Information Resources Management Journal*, *11*(1), 7-15.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rosemann, M. & Vessey, I. (2008). Toward improving the relevance of information systems research to practice: The role of applicability checks. *MIS Quarterly, 32*(1), 1-22.

Rousseau, D. M. (2006). Is there such a thing as "evidence-based management"? *Academy of Management Review*, *31*(2), 256-269.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Siponen, M. (2005). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and organization*, *15*(4), 339-375.

Siponen, M., Baskerville, R., & Heikka, J. (2006). A design theory for secure information systems design methods. *Journal of the Association for Information Systems*, 7(11), 568-592.

Siponen, M. & Tsohou, A. (2018). Demystifying the influential IS legends of positivism. *Journal of the Association for Information Systems*, in press.

Siponen, M. & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Siponen, M. & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems, 23*(3), 289-305.

Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information System Research, 1*(2), 255-277.

Straub, D. W. & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly, 22*(4), 441-469.

Tamara, D. & 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, 8*(7), 386-408.

Thagard P. (1998) Explaining disease: Correlations, causes, and mechanisms. *Minds and Machines, 8*(1), 61-78.

Thompson, B. (2002). “Statistical,” “practical,” and “clinical”: How many kinds of significance do counselors need to consider? *Journal of Counseling & Development, 80*(1), 64-71.

Vance, A., Anderson, B., Kirwan, C. & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems 15*(10), 679-722.

Venkatesh, V., Brown, S., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*(1), 21-54.

Venkatesh, V., Thong, J., & Xu, X. (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *Journal of the Association for Information Systems, 17*(5), 328-376.

Venkatesh, V., Brown, S., & Sullivan, Y. (2016) Guidelines for Conducting Mixed-methods Research: An Extension and Illustration. *Journal of the Association for Information Systems, 17*(7), 435-494.

Von Solms, R. (1998). Information security management (3): The code of practice for information security management (BS 7799). *Information Management & Computer Security, 6*(5), 224-225.

Von Solms, R. (1999). Information security management: Why standards are important. *Information Management & Computer Security, 7*(1), 50-58.

Von Solms, B. & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Zahedi, F., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals’ use and enhance their performance. *Journal of the Association for Information Systems, 16*(6), 448-484.

Appendix

Table A1. Illustrations of the Practical Problem-Solving Motivations in IS Security Research from MIS Quarterly and JAIS with Examples from Recent Descriptive Research on IS Security from JAIS and MIS Quarterly

Article	Example
Boss et al. (2015, p. 837-838), opening lines of the abstract and introduction	"Because violations of information security (ISec) and privacy have become ubiquitous in both personal and work environments, academic attention to ISec and privacy has taken on paramount importance. Consequently, a key focus of ISec research has been discovering ways to motivate individuals to engage in more secure behaviors. A key focus in information security (ISec) research is finding ways to motivate end users, employees, and consumers to improve protection of their individual and organizational information assets."
Johnston et al. (2015), introduction	"Within the modern business climate, organizations commonly suffer from threats to corporate data, information technology infrastructure, and personal computing. According to the 2007 Computer Crime and Security Survey, conducted jointly by the Computer Security Institute and the San Francisco Office of the Federal Bureau of Investigation, 46 percent of respondents reported some form of security incident during the past year (Richardson 2007). Moreover, security incidents, such as viruses, system penetrations, insider abuse, or other forms of unauthorized access continue to increase in sophistication and impact, with the average annual loss reported by U.S. companies doubling from $168,000 in 2006 to $350,424 in 2007 (Richardson 2007) . . . The present study investigates the effectiveness of persuasive messages in motivating end users to take action to secure their own computing environment."
Karjalainen & Siponen (2010, p. 519)	"To ensure that employees follow their companies' key IS security procedures, alternative approaches have been advanced in the literature, such as the use of sanctions and deterrence (Straub, 1990; Siponen, Pahnila & Mahmood, 2007)."
Keith, Shao, & Steinbart (2009), opening lines of introduction	"IT security could be enhanced by using multiple methods to authenticate users, such as combining "something you know" (e.g., a password) with "something you have" (e.g., a smartcard or token) and "something you are" (e.g., a biometric characteristic). Although the use of biometrics and smartcards is growing, passwords are still the most common, and sometimes the only authentication mechanism used by many organizations (Whitman, 2003). Therefore, it is important to find ways to improve password effectiveness."
Vance, Anderson, Kirwan, & Eargle (2014), opening lines of abstract	"Users' perceptions of risks have important implications for information security because individual users' actions can compromise entire systems. Therefore, there is a critical need to understand how users perceive and respond to information security risks."
Willison & Warkentin (2013, p. 1), opening lines of introduction	"One of the greatest concerns of IS security managers is the threat of an organizational insider. Numerous industry studies and surveys of CIOs indicate that IS security continues to be one of the top managerial concerns (Brenner 2009; CSI 2011; Deloitte 2010; Ernst & Young 2009; PwC 2008, 2010a, 2010b)."

About the Authors

Mikko Siponen is the Vice Dean for research and professor of information systems at the University of Jyväskylä. He has served more than ten years as a head of department, vice head and director of a research center. He holds a doctorate of social sciences in philosophy, M.Sc. in Software Engineering, Lic.Phil. in information systems, and PhD in information systems. He has received over €10 million in research funding from corporations and numerous other funding bodies.

Richard L. Baskerville is Regents' Professor and Board of Advisors Professor of Information Systems at Georgia State University and a professor in the School of Information Systems at Curtin University, Perth, Australia. His research regards security of information systems, methods of information systems design and development, and the interaction of information systems and organizations. Baskerville is editor emeritus of the *European Journal of Information Systems*. He is a chartered engineer and holds a BS summa cum laude from the University of Maryland, MSc and PhD from the London School of Economics, PhD (hc) from the University of Pretoria, and DSc (hc) from Roskilde University.