Original Article

Trust in Management Information Systems (MIS)

A Theoretical Model

Sarah M. Meeßen, Meinald T. Thielsch, and Guido Hertel

University of Münster

Abstract: Digitalization, enhanced storage capacities, and the Internet of Things increase the volume of data in modern organizations. To process and make use of these data and to avoid information overload, management information systems (MIS) are introduced that collect, process, and analyze relevant data. However, a precondition for the application of MIS is that users trust them. Extending accounts of trust in automation and trust in technology, we introduce a new model of trust in MIS that addresses the conceptual ambiguities of existing conceptualizations of trust and integrates initial empirical work in this field. In doing so, we differentiate between perceived trustworthiness of an MIS, experienced trust in an MIS, intentions to use an MIS, and actual use of an MIS. Moreover, we consider users' perceived risks and contextual factors (e.g., autonomy at work) as moderators. The introduced model offers guidelines for future research and initial suggestions to foster trust-based MIS use.

Keywords: trust in technology, management information systems, MIS, knowledge management, information overload

Vertrauen in Management Informationssysteme – Eine theoretisches Modell

Zusammenfassung: Digitalisierung, verbesserte Speicherkapazitäten und das Internet der Dinge vergrößern die Datenmengen in modernen Organisationen. Um diese Datenmengen zu verarbeiten, sinnvoll zu nutzen und eine Informationsüberflutung zu vermeiden, führen Organisationen Management-Informationssysteme (MIS) ein, die relevante Daten sammeln, verarbeiten und analysieren. Eine Voraussetzung für den Einsatz von MIS ist jedoch, dass Nutzer ihnen vertrauen. Aufbauend auf bestehenden Ansätzen zu Vertrauen in Automation und Vertrauen in Technologie präsentieren wir ein Modell zum Vertrauen in MIS, das konzeptuelle Unklarheiten bisheriger Vertrauenskonzepte adressiert und erste empirische Befunde in diesem Bereich integriert. Dabei differenzieren wir zwischen der wahrgenommenen Vertrauenswürdigkeit eines MIS, dem Vertrauen in ein MIS, der Absicht ein MIS zu nutzen, und der tatsächlichen Nutzung eines MIS. Zudem werden durch Nutzer wahrgenommene Risiken und kontextuelle Faktoren (z. B. Autonomie bei der Arbeit) als Moderatoren berücksichtigt. Das vorgestellte Modell bietet Leitlinien für zukünftige Forschung sowie erste Anregungen, wie eine vertrauensbasierte Nutzung von MIS unterstützt werden kann.

Schlüsselwörter: Vertrauen in Technologie, Management-Informationssysteme, MIS, Wissensmanagement, Informationsüberflutung

Today, organizations generate massive volumes of data owing to the growing computational power and digital storage capacities (Hilbert & López, 2011). Moreover, the increasing implementation of sensing technologies and digital connections between physical objects (Internet of Things; e.g., Gubbi, Buyya, Marusic, & Palaniswami, 2013) create additional masses of data. While such large amounts of data provide competitive advantages for organizations if they are systematically used and integrated in procedures and decision-making (McAfee & Brynjolfsson, 2012; Porter & Heppelmann, 2014), on the individual level, huge amounts of data can also result in excessive demands and information overload (Eppler & Mengis, 2004). Information overload can cause impaired individual performance, loss of control, and can even negatively impact users' health (Bawden & Robinson, 2009), which in turn can lead to restrictions in organizational efficacy.

One way to reduce individual workers' information overload in modern organizations is to implement management information systems (MIS) that manage large amounts of data automatically and support analysis, control, coordination, visualization, and decisions – preventing workers' information overload and improving the efficacy and quality of decision-making (e.g., Hertel et al., 2019). However, apart from such benefits, the use of an MIS can also be connected with uncertainties and risks. For instance, the "average user" is usually not the person who has programmed the MIS, nor is she/he a computer specialist in most cases. Thus, MIS users have only incomplete insights into how a specific MIS works. This

is particularly the case with increasingly complex MIS (e.g., Chen, Chiang, & Storey, 2012). Moreover, the amount of information processed by an MIS usually exceeds the capacities of a human user – this is why MIS are useful in the first place. Therefore, individual users cannot easily control the MIS's functioning or the information that is used as a basis for decision-making. Additionally, errors due to malfunctioning MIS, faultiness of information provided by MIS, or misuse of MIS by other users can lead to costly mistakes, time-consuming corrections, and damage to users' reputations and how supervisors evaluate their work performance. Thus, using MIS can entail various risks and uncertainties; thus, applying an MIS in the workplace requires a certain amount of trust in the MIS.

To date, the literature lacks a specific conceptualization of trust in MIS. Moreover, the related literature on trust in technology has not sufficiently considered conceptual differences between trust and perceived trustworthiness (Gefen, Benbasat, & Pavlou, 2008) and has not adequately specified trust on the measurement level (Söllner & Leimeister, 2013). On the basis of more general trust models (e.g., Mayer, Davis, & Schoorman, 1995), we argue that trust and trustworthiness are distinct, as they can vary independently. For instance, users might still distrust a highly trustworthy MIS if their general disposition to trust technology is low.

In this research, we define trust in MIS as the willingness to depend on and be vulnerable to an MIS without being able to monitor or control the MIS's functioning, that is, under uncertainty and risk (Gefen et al., 2008; Mayer et al., 1995). By this definition, we consider trust in MIS as an experienced state of the individual user that includes both cognitive and affective facets and that emerges and changes as a function of both the perceived trustworthiness of an MIS as well as an individual's disposition to trust technologies more generally. We define perceived trustworthiness of an MIS as the user's cognitive appraisal of the MIS as having favorable attributes in situations in which users face potential negative outcomes (Gefen et al., 2008; McKnight, Carter, Thatcher, & Clay, 2011). Perceived trustworthiness comprises users' perceptions of the reliability, functionality, helpfulness, and credibility of an MIS (McKnight et al., 2011; Thielsch, Meeßen, & Hertel, 2018). Moreover, we assume that experienced trust affects behavioral intentions of users, which in turn predict the actual use of an MIS in work processes and decisions. Notably, we consider trustful MIS use not as the naive utilization of an MIS, but rather as the reflective and deliberate use of an MIS without feeling the need for additional workarounds.

Another shortcoming in the literature to date is that behavioral intentions have often been equated with actual use of technologies, for instance, when behavioral consequences are measured through self-reports of intentions (e.g., Lankton, McKnight, & Tripp, 2015; Li, Hess, & Valacich, 2008; Thatcher, McKnight, Baker, Arsal, & Roberts, 2011). However, perceived trustworthiness, trust, behavioral intentions, and actual MIS use are not only distinct constructs, but their interrelations are also affected by different contextual conditions on various levels. For instance, the effects of trust on behavioral intentions should be moderated by risk perceptions, such as an individual user's fear of losing their reputation as respected decision-maker. Moreover, the effects of behavioral intentions on the actual use of an MIS might be moderated by general contextual factors, such as individual users' autonomy in work routines. Failing to discriminate between perceived trustworthiness, trust, behavioral intentions, and trusting behavior might lead to a neglect of the described moderating conditions, which in turn might result in an incomplete understanding of trust in MIS and potential measures to enable and enhance trusting use of MIS. In this article, we therefore offer a conceptual clarification and differentiation of the introduced constructs related to trust in MIS, and we specify moderating effects on the constructs' interrelations. In doing so, we integrate existing theoretical and empirical research on technology acceptance, trust in technology, and organizational trust.

This article makes the following contributions to the literature. To our knowledge, this is the first integrative approach for understanding trust in MIS. Of course, we do not consider trust as the only antecedent of MIS use. However, we focus on trust as a central process in this respect, integrating risk and uncertainty that are inherent to the use of complex MIS. We present a comprehensive model of trust-related processes in MIS use, including contextual moderators that are still widely unexplored. In so doing, our model provides various starting points for potential organizational measures to improve trustful MIS use at work. Moreover, based on our integrative model, we elaborate an agenda for future research. In this research, we address vocational settings in which users have certain degrees of freedom in applying the MIS and the information it provides. Please note that this is different from trust in online services, which mainly relates to private technology use and related risks, such as the theft of payment information and personal data (for a review, see Beldad, de Jong, & Steehouder, 2010). Furthermore, our model is also distinct from approaches on trust in automation and robots that focus on time-limited and safety-related work settings, such as aviation, military, and manufacturing (for reviews, see Hancock et al., 2011; Hoff & Bashir, 2015; Lee & See, 2004; Parasuraman & Riley, 1997, Parasuraman & Wickens, 2008).

Extant Models of Acceptance and Trust in Technology

In this model on trust in MIS, we integrate present models from the field of trust in technology and the broader technology acceptance tradition. As an example of the latter research perspective, the seminal technology acceptance model (TAM; Davis, 1989; Davis, Bagozzi, & Warshaw, 1989) predicts actual system use with a focus on behavioral considerations. The TAM draws on the theory of reasoned action that predicts human behavior as a manifestation of (a) beliefs about consequences of the behavior in question, (b) attitudes toward this behavior, and (c) intentions to perform this behavior (Fishbein & Ajzen, 1975). Specifically, the TAM conceptualizes perceived usefulness and perceived ease of use as predictors of use-related attitudes. These attitudes are expected to predict behavioral intentions to use a specific technology, which in turn is assumed to predict the actual use of the specific technology (Davis et al., 1989). Since results suggested that behavioral beliefs more directly affect behavioral intentions (Davis et al., 1989; Davis & Venkatesh, 1996), later versions of the TAM were modified so that attitudes were no longer considered as criteria for predicting behavioral intentions (Venkatesh & Bala, 2008; Venkatesh & Davis, 2000). Together, the TAM provides a parsimonious model to explain technology acceptance; further, it is supported meta-analytically and has been applied to various technologies, such as clinical information systems, organizational information systems, and online services (King & He, 2006).

Perhaps the most prominent example of the trust research perspective is the trust in a specific technology model introduced by McKnight and colleagues (2011). The authors focus on trusting beliefs toward technologies (i.e., beliefs that a technological artifact has favorable characteristics) that they clearly contrast with trusting beliefs toward people. In doing so, McKnight and colleagues (2011) identified trusting beliefs exclusively linked to a technology itself instead of being related to human factors in the technology's surroundings, such as technical support. In their model, McKnight and colleagues define trust in technology as the reflection of, "beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible" (McKnight et al., 2011, p. 7). Hence, McKnight and colleagues conceptualize trust through trusting beliefs that comprise reliability, functionality, and helpfulness. Empirical examinations of the model revealed that trust, measured through trusting beliefs, significantly correlated with usage intentions and self-reported use behaviors (McKnight et al., 2011).

Similar to the TAM (Davis et al., 1989), the trust in a specific technology model (McKnight et al., 2011) applies the concepts of beliefs and intentions to the processes of engaging in technology use. However, in addition to cognition (i.e., beliefs) and conation (i.e., intentions; Fishbein & Ajzen, 1975), trust is an experienced state of the individual user that includes changing affect and cognitions. Similar to the majority of online trust research (Gefen et al., 2008) and research on trust in automation (e.g., Gold, Körber, Hohenberger, Lechner, & Bengler, 2015; Jian, Bisantz, & Drury, 2000), McKnight and colleagues (2011) do not clearly distinguish between trusting beliefs about a technology's attributes and trust itself. Consequently, factors that might influence the emergence of trust as an experienced state have not been considered so far. For instance, as we will further delineate herein, the connection between perceived trustworthiness and experienced trust might become stronger the longer a technology is used.

In addition, even though McKnight (2005) originally distinguished between trusting intentions and trusting behavior, McKnight and colleagues (2011) interpreted the observed effects of perceived trustworthiness on behavioral intentions as the effects of trust on behavior. However, intentions only account for part of the variance in behavior, a phenomenon that is referred to as the *intention–behavior gap* (Sheeran, 2002) and that has also been observed in technology use (Bhattacherjee & Sanford, 2009). In our model of trust in MIS, we clearly distinguish trust from its antecedents and outcomes. In addition, we build on and extend an existing model of trust in organizations (Mayer et al., 1995), and we integrate moderators of the relations between trust and intentions as well as between intentions and behavior.

Trust in Organizations

Considering the specific context of work-related organizations and theorizing the role of both contextual and relational risk, the seminal model of organizational trust (Mayer et al., 1995) also offers a differentiated framework for conceptualizing trust in MIS. In their model that has been applied in various fields (Schoorman, Mayer, & Davis, 2007), Mayer and colleagues (1995) separate the party who trusts (the trustor) from the party who is trusted (the trustee) in order to clarify the relationality of trust. The authors assume that trust is predicated on the extent to which the trustor perceives the trustee as trustworthy. Trustworthiness comprises the trustee's ability, benevolence, and integrity. Moreover, Mayer and colleagues assume that trust is affected by the trustor's dispositional

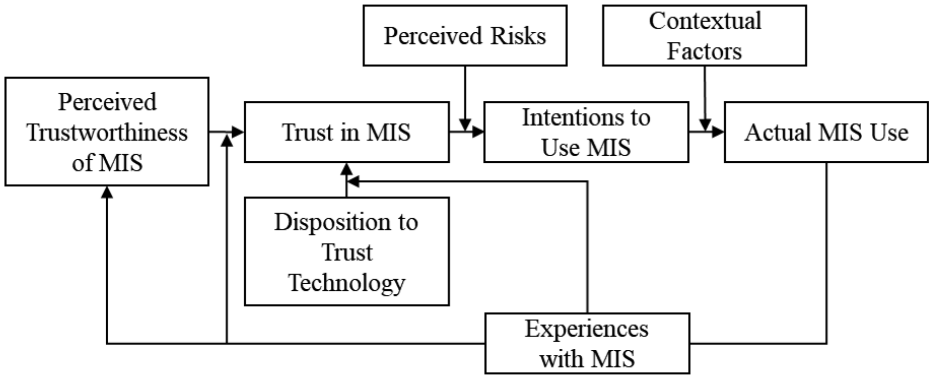

Figure 1. Theoretical model of trust in management information systems (MIS).

propensity to trust. Indeed, trusting beliefs in McKnight and colleagues' model (2011) are very similar to the concept of perceived trustworthiness in Mayer and colleagues' model (1995), as both refer to the favorable or unfavorable attributes of a trustee.

In addition, Mayer and colleagues (1995) considered risk to be inseparably linked with trust, arguing that trust becomes relevant when the trustee conducts an action relevant to the trustor; that is, when something is at stake for the trustor. In particular, the authors expect perceived risk to affect the behavioral manifestation of trust; only if trust exceeds the perceived risks will the trustor undertake risky actions. Furthermore, the authors expect that the context and outcomes of behavioral manifestations of trust influence how the trustor adjusts their prior perceived trustworthiness and trust, such that the previous outcomes feed back into further perceived trustworthiness (Mayer at al., 1995). Indeed, meta-analyses on interpersonal trust within organizational settings revealed that trust was positively correlated with task performance, citizenship behavior, and risk-taking, such as more sharing of information or delegating tasks (e.g., Breuer, Hüffmeier, & Hertel, 2016; Colquitt, Scott, & LePine, 2007).

By distinguishing between perceived trustworthiness, trust, perceived risks, and behavioral outcomes, the model of trust in organizations (Mayer at al., 1995) considers the constructs' singularities and allows one to explore moderators that specifically affect the constructs' interrelations. Therefore, this model offers a starting framework for trust in MIS. However, Mayer and colleagues (1995) did not distinguish between trust and related behavioral intentions, potentially neglecting factors that might influence the extent to which intentions result in actual behavior. In our model of trust in MIS, we integrated perceived behavioral control (e.g., Ajzen, 1985) as another central building block.

A Theoretical Model of Trust in MIS

Following the described considerations, we conceptualize individuals' trust in MIS by integrating various theoretical concepts. Specifically, among the predictors of MIS use, we distinguish between users' perceptions of MIS trustworthiness, their trust in the MIS, and their behavioral intentions to use the MIS. Figure 1 shows our proposed model of trust in MIS. In the following, we define the different constructs of the model and integrate them into current research. Moreover, we offer concrete propositions for the concepts' interrelations.

Perceived Trustworthiness of MIS

Following the general structure of the model of organizational trust (Mayer et al., 1995), we consider potential users of an MIS as trustors (i.e., the entity that makes her-/himself vulnerable) and the MIS as trustee (i.e., the entity that can potentially harm the trustor). Thus, the extent to which users perceive an MIS as trustworthy should be one main predictor of their experienced level of trust in the MIS. However, we deliberately distinguish trustworthiness perceptions and trust because perceived trustworthiness depicts the appraisal of an MIS's characteristics, whereas trust describes an emergent state of an individual willing to depend and to make oneself vulnerable (Gefen et al., 2008; Mayer et al., 1995). While both constructs are positively related, the relationship is not deterministic and can be qualified by moderating factors such as specific experiences with the MIS over time.

Related distinctions between perceived trustworthiness and trust in technology have been made in the field of e-commerce: Komiak and Benbasat (2004) offered a distinction between *cognitive trust*, which can be seen as similar to perceived trustworthiness, and *emotional trust*, described as, "the trustor's feeling toward the behavior of relying on the trustee" (Komiak & Benbasat, 2006,

p. 944). In an experimental study, the authors found that both cognitive trust and emotional trust had positive effects on intentions to adopt a recommendation agent. Moreover, emotional trust partially mediated the effect of cognitive trust on the intention to adopt the recommendation agent (Komiak & Benbasat, 2006). These results are in line with our proposed distinction between perceived trustworthiness and trust, with the assumed partial mediation process between perceived trustworthiness, trust, and behavioral consequences. However, our model considers trust not exclusively as an affective state but as an experienced state that includes both affective and cognitive facets (for an initial operationalization, see the trust items used in Thielsch et al., 2018).

In general, we assume that users are more willing to rely on an MIS and to make themselves vulnerable to an MIS when they perceive the MIS to predictably and adequately fulfil their needs to master a situation. Consequently, users' perceptions of the trustworthiness of an MIS should affect their experienced trust in the MIS. We further specify four different facets of trustworthiness perceptions that are grounded both in more general theoretical accounts (i.e., McKnight et al. 2011) as well as more recent empirical research (Thielsch et al., 2018). McKnight and colleagues (2011) considered three factors to be relevant trustworthiness perceptions of technologies: the extent to which a piece of technology has features that allow users to fulfil their intended tasks (functionality), the extent to which the technology operates in a continual and accurate manner (reliability), and the extent to which the technology provides help for the user (helpfulness). These factors have been widely adopted in information systems research in order to measure trust and its effects on the intention to explore, the intention to trust, or the intention to continue to use a specific information system (e.g., Lankton et al., 2015; Thatcher et al., 2011). Complementing and further extending these factors, Thielsch and colleagues (2018) applied an explorative approach to examine antecedents and consequences of trust in information systems at work using the critical incident interview technique (Flanagan, 1954). Their results suggest that users assess the trustworthiness of an MIS not only by considering features of the MIS itself, but also by assessing the credibility of the information that the MIS provides. Thielsch and colleagues (2018) successfully validated the explorative findings in a second study using a quantitative approach. Users may assess the trustworthiness of an MIS before their first use, for instance, based on conversations with colleagues, supervisors, or the technical support staff, or from their first impression of the user interface. Together, we propose:

Proposition 1: Individuals' trust in an MIS is predicted by their perceived trustworthiness of the MIS (i.e., subjective perceptions of functionality, reliability, helpfulness, and credibility of provided information).

Disposition to Trust Technology

As in trust processes more generally, we assume trust in a specific MIS also to be affected by the trustor's stable dispositions. Mayer and colleagues (1995) defined dispositional factors as the "general willingness to trust others" (p. 715). More specifically in the context of technologies as trustees, McKnight and colleagues (2011) defined a person's propensity to trust technology as "the[ir] general tendency to be willing to depend on technology across a broad spectrum of situations and technologies" (McKnight et al., 2011, p. 7). The authors operationalized this concept through two factors: first, a person's tendency to assume that technologies have favorable attributes (faith in general technology), and second, a person's assumption that they can rely on technology in general (trusting stance in general technology). However, in later research, a person's propensity to trust was operationalized exclusively through their trusting stance (Lankton et al., 2015). Initial empirical results indicated that such disposition to trust technology significantly affected trusting intentions and intentions to continue using a specific technology (Lankton et al., 2015).

In line with the general structure of trust-related processes outlined by Mayer and colleagues (1995), we argue that users' disposition to trust technology affects the extent of their experienced trust in MIS. Users who generally tend to trust different technologies in various situations should experience higher degrees of trust in an MIS, whereas users who are generally unwilling to depend on technology should experience lower trust in an MIS. Thus, we propose:

Proposition 2: Individuals' trust in an MIS is predicted by their disposition to generally trust technology.

Notably, trust in automation research (e.g., Lee & See, 2004) as well as the organizational trust model (Mayer et al., 1995) considered trust as an attitude. However, given that attitudes are rather stable (Fishbein & Ajzen, 1975), such a conceptualization of trust makes it difficult to represent the dynamic and reactive aspects of trust emergence and development over time. Therefore, we consider trust-related attitudes as part of individuals' disposition to trust technology in general (see Figure 1), complementing other more stable dispositional influences on trust such as personality factors (e.g., extraversion, conscientiousness, and agreeableness; Furumo, de Pillis, & Green, 2008). By contrast, we consider trust as an

emerging state, experienced by the trusting individual, and constantly influenced by the various factors considered. For instance, users' trust in an MIS is likely to decrease as soon as an MIS works unreliably (e.g., after a defective software update), and trust should gradually increase again after programming errors have been fixed.

Trust in MIS, Behavioral Intentions, and Actual Use of MIS

Having established the concept of trust in MIS and its predictors, we now turn to the consequences of trust, differentiating trust from behavioral intentions and the actual use of an MIS. In online trust research, trust has widely been defined as the willingness to depend on someone or something (e.g., Gefen et al., 2008). Moreover, scholars in general have integrated behavioral intentions into their conceptualization of trust or referred to trust as a behavioral intention (e.g., Gefen et al., 2008; Mayer et al., 1995; McKnight et al., 2011). However, we argue that it is important to distinguish trust from behavioral intentions for two reasons. First, trust in general, and trust in MIS more specifically, becomes relevant when the trustor's interests are at risk (Mayer et al., 1995), whereas behavioral intentions do not require potential vulnerability as a necessary precondition but precede any kind of deliberate behavior (Fishbein & Ajzen, 1975). Second, trust in MIS and behavioral intentions to use an MIS do not share the same antecedents. As argued earlier, trust in MIS is assumed to be based on trustworthiness perceptions of the MIS and on the general disposition to trust technology, whereas behavioral intentions are also affected by beliefs toward the behavior in question and social norms (e.g., Venkatesh & Davis, 2000). According to the theory of reasoned action, the intention to perform a certain behavior can be considered as the subjective likelihood to conduct a certain behavior (Fishbein & Ajzen, 1975). For MIS use, we assume that trust in MIS is only one out of several factors that positively affect one's intention to use an MIS. Nevertheless, if users are willing to depend on and be vulnerable to an MIS, they should have a greater intention to use it.

Proposition 3: Individuals' trust in an MIS partly predicts their behavioral intentions to use the MIS.

Moreover, we assume that intentions to use an MIS enhance the likelihood that users actually use the MIS. Please note that this prediction is not trivial because behavioral intentions are not the only predictors of actual usage behavior (e.g., Bhattacherjee & Sanford, 2009). Other factors that affect technology use at work are, for instance, developed habits and routines, prescribed work processes, or legal regulations. Therefore, we assume that behavioral intentions only partly predict actual use of MIS:

Proposition 4: Individuals' behavioral intentions to use an MIS partly predict their actual use of the MIS.

Perceived Risks and Contextual Constraints as Moderating Conditions

Mayer and colleagues (1995) considered risk in two different ways. First, they integrated risk in the trust definition because they described the "willingness to make oneself vulnerable" also as the willingness to take risks. Second, the authors considered perceived risk to be relevant for the manifestation of trust, that is, for the translation into actual risk-taking behavior. Applied to trust in MIS, the former includes risks inherent in the relation between a user and an MIS, whereas the latter refers to contextual conditions and comprises the trustor's belief in the likelihood of gains or losses due to these perceived contextual risks (see Mayer et al., 1995). For instance, even when users trust an MIS (because the MIS is perceived as trustworthy and dispositional trust factors are high), they should not intend to rely on the MIS if context conditions are too risky (e.g., when potential mistakes are too costly, or when the management disapproves of using technologies). Consequently, we contend that perceived risks due to context conditions represent a crucial moderator for the effect of trust on behavioral intentions to use MIS. Moreover, we argue that perceived risks are particularly relevant for the intention formation process when users deliberately consider gains and losses of MIS usage.

Trust and related risks have been examined in e-commerce studies on private usage of (mainly commercial) online services, in which websites or recommendation agents were the trustees. Results have indicated that e-commerce customers perceived risks particularly with regard to theft of payment details and personal information (e.g., Kim, Ferrin, & Rao, 2008; Liebermann & Stashevsky, 2002). In work-related settings, different risks are to be considered when workers seek to make a living and to fulfil personal needs (e.g., growth, achievement, self-esteem) and social needs (e.g., relatedness, affiliation; see Haslam, Powell, & Turner, 2000). Prominent examples for work-related risks are potential losses regarding social status or career progress.

Social status can be defined as, "respect, admiration, and voluntary deference individuals are afforded by others" (Anderson, Hildreth, & Howland, 2015, p. 1) and represents an important part of workers' self-esteem. If this social status is threatened when an MIS is used, for instance, when supervisors are overtly critical when errors

occur, the intention to rely on an MIS should decrease even if the MIS is perceived to be trustworthy.

Risks regarding career progress relate to negative repercussions for users' careers. For instance, if users are held accountable for decisions made based on an MIS, the intention to rely on the MIS should decrease even if the MIS itself is trusted. In such situations, users are more likely to apply workarounds, for example, by running extensive double-checks with source data. Together, the effects of experienced trust in an MIS on the intention to use the MIS is assumed to be qualified by contextual conditions that increase or decrease the potential risks related to MIS use. Thus, we postulate:

Proposition 5: The relation between users' trust in an MIS and their intention to use the MIS is moderated by their perception of related risks when using the MIS: Higher perceived risks (potential losses) reduce the effect of users' trust on users' intentions to use the MIS.

In addition to moderating effects of users' risk perceptions on the relation between trust in an MIS and deliberate intentions to use the MIS, we also consider moderating conditions of the relation between deliberate intentions to use an MIS and the actual usage (i.e., behavior) of the MIS (see Figure 1). In general, the intention–behavior link can be influenced by numerous factors, such as type and properties of intentions and behavior, personality factors, or action control and habits (e.g., Sheeran, 2002).

Applied to our model of trust in MIS, trust-based intentions to use an MIS are only one out of many factors that determine the actual usage of an MIS. Other influencing factors do not directly relate to experienced trust of the user but reflect contextual conditions such as users' control and autonomy at work, supervisory instructions, or social norms and work routines. These factors not only directly affect the likelihood of MIS use, but they also moderate the strength of the relation between users' trust-based intentions to use an MIS and actual usage behavior. For instance, perceived behavioral control can affect usage behavior both directly and indirectly through trust-based intentions (Ajzen, 2002). More generally, we assume that the relation between trust-based intentions to use an MIS and actual MIS use is qualified by environmental factors that simplify or impede the voluntary control of the individual user. Thus, we propose:

Proposition 6: The relation between users' intentions to use an MIS and the actual use of the MIS is moderated by contextual factors: Factors facilitating users' control increase the relation between users' intention to use an MIS and actual usage of the MIS.

MIS Use and Experiences With the MIS

In our proposed model of trust in MIS, actual MIS use is the main outcome variable, where actual MIS use reflects the secure dependence or reliance on the MIS instead of trying to control the MIS (McKnight, 2005). That is, actual MIS use refers to the application of an MIS in organizational work processes without individual users conducting unnecessary workarounds or consulting additional information sources. However, actual MIS use is not only considered as an outcome but also as a precursor for following trustworthiness assessments. When using an MIS, individuals gain experience with the MIS, which enables further evaluations and re-evaluation of the trustworthiness of the MIS. Thus, MIS use can change perceived trustworthiness in repeated feedback circles:

Proposition 7: The evaluation of an MIS during usage affects the perceived trustworthiness of an MIS in subsequent usages.

Moreover, as proposed by Schoorman and colleagues (2007), dispositional factors with respect to trust should be particularly relevant in the initial phases of trust building, when trustors have only few personal experiences with the trustee. In our model of trust in MIS, we assume that users rely on more general attitudes and dispositions when having only few or no personal experiences with an MIS. Such general attitudes and dispositions might also influence users' initial impression of an MIS's interface, or information about the MIS from others. By contrast, systematic assessments of the trustworthiness of an MIS should become more relevant over time when users gain more personal experience with the MIS. Together, we assume that experiences with an MIS moderate the relative impact of MIS trustworthiness perceptions and dispositions to trust technology:

Proposition 8a: The effect of users' trustworthiness perceptions on trust in an MIS is moderated by users' experience with the MIS: More experience with the MIS increases the effect of perceived trustworthiness on trust.

Proposition 8b: The effect of users' disposition to trust in technology on trust in an MIS is moderated by users' experience with the MIS: More experience with the MIS decreases the effect of users' disposition to trust technology.

Summary and Discussion

In this article, we introduce a model of trust in MIS that integrates and extends current theories on trust and technology acceptance, as well as initial empirical results. We understand trust in MIS as an experienced state, defined as the willingness to depend on and be vulnerable

to an MIS. This definition distinguishes trust from trustworthiness perceptions of an MIS, mere attitudes toward technologies, and behavioral intentions to use an MIS. As such, our model goes beyond approaches that are less clear about the distinction between these constructs, responding to related calls for more conceptual precision in this emerging field (e.g., Gefen et al., 2008).

This model of trust in MIS considers users' trustworthiness perceptions of an MIS and their disposition to trust in technologies as antecedents of trust. We propose that trust enhances users' behavioral intentions to use MIS and that behavioral intentions thereafter inform actual MIS use. Furthermore, we assume a feedback loop from concrete experiences that users have through actual MIS use on trustworthiness perceptions as well as on the impact that trustworthiness perceptions and disposition to trust have on trust. We also expect that users' perceptions of risks (Mayer et al., 1995), for instance, potential losses in social or vocational status within the work group or organization, moderate the effect of trust on behavioral intentions. Moreover, drawing on approaches that explain behavior in general (Ajzen, 1985, 2002) and in automation reliance (Lee & See, 2004) as well as extending trust in technology (e.g., McKnight et al., 2011) and technology acceptance models (e.g. Davis et al., 1989), we assume that contextual factors moderate the translation of trust-based intentions to use the MIS into actual MIS use.

The presented model can be contrasted with current approaches for trust in online services (e.g., Beldad et al., 2010; Gefen et al., 2008) and trust in automation (e.g., Lee & See, 2004) by addressing trust in MIS applied in management settings. This includes specific characteristics of MIS use at workplaces: Whereas users of online services perceive vulnerabilities that are related to potential misuse of their personal data and payment information, MIS users perceive vulnerabilities that are related to their job performance and their status at work. Trust in automation research examines automated processes that are characterized by time limitations and safety regulations (Parasuraman & Wickens, 2008); By contrast, the application of MIS in management processes subtends higher degrees of volitional control.

Research Implications

The presented model provides interesting guidelines for future research. The proposed distinctions between perceived trustworthiness, trust in MIS, and behavioral intentions to use MIS need to be examined empirically, together with considered moderating factors. Moreover, measuring trust in MIS reliably and distinctly from related constructs is still an unresolved topic. Even though scales are provided for measuring trustworthiness factors (e.g., McKnight et al., 2011), emotional trust (Komiak & Benbasat, 2006) and behavioral intentions (e.g., Venkatesh, Morris, Davis, & Davis, 2003), more research is needed to examine whether these scales truly distinguish between the related concepts. To the best of our knowledge, no extensively tested scale is available that applies to the integral psychological state of trust in MIS as it is proposed in the current work. The need for appropriate scales and measurement models is emphasized by measurement model misspecifications that have previously been identified in information system trust research (Söllner & Leimeister, 2013). The moderating effect of perceived risks and contextual factors represents another starting point for future research. Further research is also needed to assess what exactly constitutes perceived risks and contextual factors.

For reasons of parsimony, we focused on the main relationships between the concepts in our proposed model. Nevertheless, additional relationships are conceivable and might be addressed in further investigations. For instance, users' disposition to trust might moderate experiences with an MIS. Users with low disposition to trust in technology may focus on negative information about the MIS, leading to a more biased perception of MIS's trustworthiness.

Moreover, differentiating trust from behavioral intentions allows for the analysis of specific trust effects that go beyond mere MIS use. For instance, recent empirical data have shown that trustful usage of MIS at work was accompanied by significantly higher levels of well-being, performance, and post-usage satisfaction as compared with distrustful usage of MIS (Thielsch et al., 2018). These results suggest that trust is not only relevant for actual MIS use but can also contribute to less strenuous working conditions. Given the constantly increasing volumes of data in modern organizations, more research is needed on health determinants that are related to MIS use and to trusting in MIS. As an initial example, a recent experimental study showed that MIS use not only improved the well-being of its users and enhanced individual performance, but it also liberated mental resources for unrelated additional tasks (Hertel at al., 2019). More research is needed in order to clarify the relevance of trust in the related MIS in terms of enhancing performance and well-being.

Additionally, further investigations are needed on the nature of trust. In our proposed model, we understand trust as an experienced state that constantly reacts to trustworthiness perceptions and changes in the course of actual MIS use. With this conceptualization, we draw on the call for more *temporalism* in applied psychology (Roe, 2008). Still, little research has been conducted on the dynamic properties

of trust. Longitudinal studies are desirable, including studies that examine trust in MIS at various points, for example, during a working day. Indeed, the proposed impact of actual MIS use and the related change in perceived trustworthiness and consequently in trust would entail an analysis of trust in various stages of use.

In general, the boundary conditions of the presented model need to be examined. Even though we determined boundary conditions by focusing on vocational management settings, broader contextual factors, such as culture (Leidner & Kayworth, 2006), merit further examination. While the presented model focuses on trust, distrust may involve additional influencing factors or different processes (e.g., Seckler, Heinz, Forde, Tuch, & Opwis, 2015, Thielsch et al., 2018) providing another starting point for further investigation.

Implications for Practitioners

The proposed model entails three major practical implications to enhance MIS use and, thus, to reduce overload through growing amounts of organizational data: enabling trust, reducing perceived risks, and diminishing contextual constraints. First, in order to enable trust, an MIS has to be (perceived as) reliable, functional, and helpful and to provide credible information. Thielsch and colleagues (2018) offer practical implications for enhancing trust in information systems at work, as well as for avoiding distrust. Their implications comprise system quality, information quality, service quality, context, and persons involved. In addition, experiences with the MIS and realistic information about the MIS's favorable attributes can lower the potentially biased impact of dispositional trust.

Second, reducing the perceived risks of the MIS increases the probability that trust will result in intentions to use the MIS. Therefore, contextual conditions of MIS use such as leadership behavior or organizational policies should be reconsidered and adapted if necessary. A context in which potential personal gains exceed potential personal losses should lower perceived risks and therein make actual MIS use more probable.

Third, in order to strengthen the effects of trust-based intentions to use the MIS on actual MIS use, organizations might consider contextual factors that impede MIS use during the MIS's implementation, such as to assure easy access and use of the MIS (e.g., Venkatesh, 2000) or to train and support users. In addition, MIS use might be positively influenced by increasing users' control during the implementation process, through involving them in the acquisition, configuration, and potential changes of MIS relevant to their workplace. Moreover, organizations might review and redefine decision-making practices and support from top management (e.g., McAfee & Brynjolfsson, 2012).

Conclusion

Digitalization and the Internet of Things are progressing, and the amounts of data in and around organizations are increasing. MIS represent promising applications that can deliver benefits by easing worker overload in the face of growing volumes of organizational data. While trust in an MIS represents an essential precondition for actual MIS use, perceived trustworthiness, perceived risks, and contextual factors represent the essential key components in translating this trust into actual MIS use. The proposed model integrates these key components, thus providing orientation and implications for both research and practice.

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action Control* (pp. 11 – 39). Berlin, Heidelberg, Germany: Springer.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32*, 665 – 683.

Anderson, C., Hildreth, J. A. D., & Howland, L. (2015). Is the desire for status a fundamental human motive? A review of the empirical literature. *Psychological Bulletin, 141*, 574 – 601.

Bawden, D., & Robinson, L. (2009). The dark side of information: Overload anxiety and other paradoxes and pathologies. *Journal of Information Science, 35*, 180 – 191.

Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the Faceless and the Intangible? A literature review on the antecedents of online trust. Computers in Human Behavior, 26, 857 – 869.

Bhattacherjee, A., & Sanford, C. (2009). The intention-behaviour gap in technology usage: The moderating role of attitude strength. *Behaviour & Information Technology, 28*, 389 – 401.

Breuer, C., Hüffmeier, J., & Hertel, G. (2016). Does trust matter more in virtual teams? A meta-analysis of trust and team effectiveness considering virtuality and documentation as moderators. *Journal of Applied Psychology, 101*, 1151 – 1177.

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly, 36,* 1165 – 1188.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trustworthiness, and trust propensity: A meta-analytic test of unique relationships with risk taking and job performance. *Journal of Applied Psychology, 92*, 909 – 927.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*, 319 – 339.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*, 982 – 1003.

Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: Three experiments. *International Journal of Human-Computer Studies, 45*, 19 – 45.

Eppler, M., & Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. *Information Society, 20*, 325 – 344.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin, 51*, 327 – 358.

Furumo, K., de Pillis, E., & Green, D. (2008). Personality influences trust differently in virtual and face-to-face teams. *International Journal of Human Resources Development and Management, 9* (1), 36 – 58.

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems, 24*, 275 – 286.

Gold, C., Körber, M., Hohenberger, C., Lechner, D., & Bengler, K. (2015). Trust in automation – before and after the experience of take-over scenarios in a highly automated vehicle. *Procedia Manufacturing, 3*, 3025 – 3032.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*, 1645 – 1660.

Hancock, P. A., Billings, D. R., Schaefer, K. E., Chen, J. Y. C., de Visser, E. J., & Parasuraman, R. (2011). A meta-analysis of factors affecting trust in human-robot interaction. *Human Factors, 53*, 517 – 527.

Haslam, S. A., Powell, C., & Turner, J. (2000). Social identity, self-categorization, and work motivation: Rethinking the contribution of the group to positive and sustainable organisational outcomes. *Applied Psychology, 49*, 319 – 339.

Hertel, G., Meeßen, S. M., Riehle, D., Thielsch, M. T., Nohe, C., & Becker, J. (2019). Directed forgetting in organisations: The positive effects of decision support systems on mental resources and well-being. *Ergonomics, 62,* 597 – 611.

Hilbert, M., & López, P. (2011). The world's technological capacity to store, communicate, and compute information. *Science, 332*, 60 – 65.

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors, 57*, 407 – 434.

Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics, 4*, 53 – 71.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*, 544 – 564.

King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. *Information & Management, 43*, 740 – 755.

Komiak, S. Y., & Benbasat. I. (2004). Understanding customer trust in agent-mediated electronic commerce, web-mediated electronic commerce, and traditional commerce. *Information Technology and Management, 5*, 181 – 207.

Komiak, S. Y., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *Management Information Systems Quarterly, 30*, 941 – 960.

Lankton, N., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association of Information Systems, 16*, 880 – 918.

Leidner, D. E., & Kayworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, *30*, 357 – 399.

Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage. *Qualitative Market Research: An International Journal*, *5*, 291 – 300.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors, 46*, 50 – 80.

Li, X., Hess, T., & Valacich, J. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *Journal of Strategic Information Systems, 17*, 39 – 71.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*, 709 – 734.

McAfee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. *Harvard Business Review, 90*, 60 – 68.

McKnight, D. H. (2005). Trust in information technology. In G. B. Davis (Ed.), *The Blackwell encyclopedia of management (Management information systems Vol. 7.,* pp. 329 – 331). Malden, MA: Blackwell.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS), 2*, 12.

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, *39*, 230 – 253.

Parasuraman, R., & Wickens, C. D. (2008). Humans: Still vital after all these years of automation. *Human Factors, 50*, 511 – 520.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, *92*, 64 – 88.

Roe, R. A. (2008). Time in applied psychology. The study of "What happens" rather than "What is". *European Psychologist, 13*, 37 – 52.

Sheeran, P. (2002). Intention-behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*, 1 – 36.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review, 32*, 344 – 354.

Seckler, M., Heinz, S., Forde, S., Tuch, A. N., & Opwis, K. (2015). Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior, 45*, 39 – 50.

Söllner, M., & Leimeister, J. M. (2013). What we really know about antecedents of trust: A critical review of the empirical information systems literature on trust. In D. Gefen (Ed.), *Psychology of trust: New research* (pp. 127 – 155). New York, NY: Nova Science Publishers.

Thatcher, J. B., McKnight, D. H., Baker, E. W., Arsal, R. E., & Roberts, N. H. (2011). The role of trust in postadoption IT exploration: An empirical examination of knowledge management systems. *IEEE Transactions on Engineering Management, 58*, 56 – 70.

Thielsch, M. T., Meeßen, S. M., & Hertel, G. (2018). Trust and distrust in information systems at the workplace. *PeerJ, 6, e5483.*

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*, 342 – 365.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*, 273 – 315.
Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*, 186 – 204.
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*, 425 – 478.

History
Received May 9, 2018
Revision received November 16, 2018

Acknowledgments
We would like to thank the anonymous reviewers for their helpful comments.

Funding
This research was supported by a grant from the Deutsche Forschungsgemeinschaft to Guido Hertel (He 2745/16-1).

ORCID
Sarah M. Meeßen
https://orcid.org/0000-0002-5643-0814

Sarah M. Meeßen
Prof. Dr. Meinald T. Thielsch
Prof. Dr. Guido Hertel
Department of Psychology
Organisational and Business Psychology
University of Münster
Fliednerstraße 2
48149 Münster
Germany
sarah.meessen@uni-muenster.de