Perceived Information-Based Vulnerability of Enterprise Information Systems: Concept, Antecedents, and Outcomes

Research-in-Progress

Sarah Träutlein
Technische Universität Darmstadt
Chair of Information Systems | Software Business & Information Management
Hochschulstraße 1, D-64289
Darmstadt, Germany
traeutlein@is.tu-darmstadt.de

Jin P. Gerlach
Technische Universität Darmstadt
Chair of Information Systems | Software Business & Information Management
Hochschulstraße 1, D-64289
Darmstadt, Germany
gerlach@is.tu-darmstadt.de

Abstract

Many of today's enterprise information systems require employees to make correct information about their skills, activities, or opinions available to their organization. In this research, we argue that the success of these systems depends strongly on the relationship quality between the employees and their employers. Based on principal–agent and psychological contract theory, we propose a conceptual framework that features a user’s perceived information-based vulnerability (PIBV) of a system: a construct that reflects a user’s perceptions that information entered into a system could be used in an opportunistic manner by the employer. Our framework suggests that employees who fear that a system serves as potential data source that informs the organization about their abilities and fulfillment of duties will reduce their quality usage. Outcomes of this research could help understand the peculiarities of revealing enterprise information systems (REIS) which depend on employees revealing skills, activities, or opinions to their employer.

Keywords: Principal–Agent Theory, Psychological Contract Theory, Perceived Information-Based Vulnerability, Sensitive Employee Data, System Usage
Introduction

Organizations are investing considerable amounts of time and money in implementing information systems such as enterprise social networks, knowledge management systems, or mobile apps, to enhance employee performance and to increase organizational success (e.g., Koch et al. 2012; Treem and Leonard 2012). While the usage of many information systems is guided by straightforward workflows, the true value of certain others depends on the readiness of their users to supply information about themselves and their activities (Eisenberg and Witten 1987; Gibbs et al. 2013). Such systems depend on employees who share their professional skills (Koch et al. 2012, 2013; Treem and Leonard 2012), locations (Junglas and Watson 2008), status (DiMicco et al. 2008; Koch et al. 2013), activities, thoughts, or opinions (Denyer et al. 2011; Hurbean and Fotache 2013; Koch et al. 2013). Examples for current systems which require employees to reveal such information are enterprise social systems (e.g., internal social networks, blogs, and wikis), employee feedback systems, or location-based mobile enterprise apps (Berghaus and Back 2014; Gibbs et al. 2013; Hurbean and Fotache 2013; Mokbel et al. 2007). It is important for companies to understand what prevents and motivates employees to disclose honest information into these systems about themselves, otherwise the investment might have failed its purpose. As we will argue below, reasons for such a behavior might not only stem from the system and its characteristics itself but from the relationship an employee perceives with its company. Employees who, for example, perceive that disclosed information might be used to harm them will not use the system or even might react with a destructive attitude. Therefore, the present research suggests a new perspective on these enterprise information systems which have in common that their value for the company depends on users’ readiness to provide truthful information about themselves.

What kind of perspective do we propose and why is such a perspective valuable? We argue that for these kinds of systems, it is even more important to investigate the quality of usage when assessing their success than it is for other classes of IS, as it depends on users who provide both sensitive as well as correct information about themselves and their work within these systems. For example, the success of an enterprise social system is questionable if employees insert what they think will present them favorably in front of their managers and companies and therefore use these systems for impression management (Birnholtz et al. 2012; Gibbs et al. 2013). As another example, consider an HR 360 degree feedback system that will not fulfill its purpose if users do not share their honest and open opinion how their managers are running the organization but rather fear that criticism might be traced back to them. At the same time, high quality usage of these systems should be hard to enforce and control as the sincerity and correctness of user input cannot be determined easily by objective criteria. In sum, the success of these systems should strongly depend on the quality of information entered by employees about themselves. For the ease of argumentation throughout this research-in-progress, we use the label “Revealing Enterprise Information Systems” (REIS)—suggesting that information within these mentioned enterprise information systems is more or less revealing for the user who provides it.

In this research, we take a closer look at REIS and argue that their unique characteristics determine their success in a particular way. As REIS depend on users’ sharing of revealing information about themselves with their employer, the quality of REIS usage should be closely related to the relationship quality between employees and their organizations. To better understand the nature of this class of enterprise information systems, we refer to the principal–agent perspective, which has been used to explain exchange relationships among self-interested parties with different objectives while uncertainty and imperfect information balance are prevalent (Eisenhardt 1989). In socio-economic systems, principal-agent theory is used to describe exchange relationships where information asymmetry, anxiety for opportunism, as well as limited rationality are present (Milgrom and Roberts 1992). It illustrates an employer’s (i.e., principal’s) uncertainty about the characteristics and actions of its employees (i.e., agents) (Eisenhardt 1989; Rousseau and McLean Parks 1993). Revealing information within REIS means that a user actively reduces this information asymmetry in favor of the employer by disclosing his or her activities, skills, or opinions. Principal–agent theory further assumes that both principal and agent act self-interested and opportunistically (Eisenhardt 1989) which means that employees who reveal information within REIS must trust that this information is not used against them. Therefore, the quality of the employee–employer relationship, which is subject of psychological contract theory (e.g., Morrison and Robinson 1997; Rousseau 1989; Rousseau and McLean Parks 1993) should determine an employee’s anticipation of opportunistic behavior and thus the quality of REIS usage. To get a better understanding of the role of employees’ readiness to provide truthful personal information and the resulting consequences, we refer to
psychological contract theory, which describes a subjective expectation detained in a mental model of an employer regarding his expectations how his employer should behave and act toward the employee and his environment (Morrison and Robinson 1997).

In order to conceptualize this rationale, we propose a new construct—the perceived information-based vulnerability (PIBV) of systems—which captures a user’s perceptions that information entered into a system can be used in an opportunistic manner by the employer. As PIVB displays a perceived system characteristic, organizations can evaluate IS they want to implement in order to get a feel for their future success. Over the course of this research, we seek to propose and empirically test antecedents and outcomes of PIVB and supply a validated measure for this newly developed construct. Going further, we present both principal–agent and psychological contract theory which serve as theoretical foundation for our research. Afterwards, we provide a more detailed elaboration on the nature and definition of REIS. In the subsequent chapter, we define the construct of PIVB and situate it within a nomological net. Next, we briefly illustrate our plans for data collection to validate PIVB and test our propositions. We conclude with a summary of the potential contributions of our research.

Theoretical Background

IS research has accumulated an impressive body of knowledge predicting and explaining system acceptance, usage, and success (e.g., Davis 1989; DeLone and McLean 2003; Venkatesh et al. 2003). A vast stream of research has thereby evolved around the technology acceptance model (TAM), the unified theory of acceptance and use of technology (UTAUT), and their extensions (e.g., Davis 1989; Venkatesh and Bala 2008; Venkatesh et al. 2003). While these efforts have considerably broadened our perspective on individuals’ usage of technologies, an aspect which still requires attention is presented by the quality or effectiveness of system use (e.g., Barki et al. 2007; Burton-Jones and Grange 2012; Burton-Jones and Straub Jr. 2006). We argue that this is especially relevant for REIS as their value can only be derived when assessing the particular usage quality. If employees are providing false information or engage in impression management, the true value of REIS might not be achieved.

In the following subsections, we present two theories that can help explain how the relationship quality between an employee and an employer can determine how employees perceive REIS and therefore provide quality information within these systems. Principal–agent theory serves as a general framework to underscore the challenges arising from information asymmetries between an organization and its workers and the role of IS to reduce these asymmetries, as well as the limited rationality of users when it comes to the perceived possibility of employers to act opportunistically and against the self-interest of employees. Psychological contract theory explains how an employee’s perceived relationship quality toward his or her employer determines which behaviors he or she expects from the organization and how these expectations can affect work-related behavior such as REIS usage. Therefore, based on both theories it is possible to derive possible outcome behaviors when using REIS.

Principal–Agent Theory

As outlined above, employees might think twice before revealing information within REIS. Such hesitation can be better understood if viewed from the perspective of principal–agent theory. Principal–agent theory has been used by many to explain the relationships between employees, their organizations, and the dynamics between both parties (e.g., Eisenhardt 1989; Rousseau and McLean Parks 1993). The theory assumes that a principal (e.g., an employer) hires an agent (e.g., an employee) to perform on behalf of the principal (e.g., Eisenhardt 1989; Jensen and Meckling 1976; Pavlou et al. 2007). Principal–agent relationships are further characterized by conflicting desires and information asymmetries between both parties which are said to act opportunistically and with limited rationality. This creates two problems from the principal’s point of view. First, the principal may lack information about the agent’s actual characteristics (e.g., skills) and risks choosing an agent who performs worse than assumed (i.e., adverse selection). Second, the principal might not be able to observe the agent’s true behaviors and is not able to validate if the agent has acted appropriately (i.e., moral hazard). To counter these issues, the principal can engage in screening or monitoring activities or rely on signals sent by the agent and thereby try to learn more about the true characteristics and behaviors of the agent (e.g., Eisenhardt 1989; Pavlou et al. 2007; Rousseau and McLean Parks 1993).
One possibility how an organization can monitor and control the performance and behavior of its workforce is to invest in information systems which reveal the characteristics and actions of employees (e.g., Eisenhardt 1989; Allen et al. 2007). Many recent IS offer the possibility to reveal what employees know and what they are doing at work as conversations are persisted within enterprise social networks and mobile apps are able to track the movement of employees when installed on a smartphone. Information revealed within REIS can therefore help reduce information asymmetries in favor of the company and therefore create a power advantage for the employer. Making use and exploiting existing and potentially substantial employee information might be tempting for companies (Sewell and Barker 2006). Doing so, however, may evoke a feeling of uncertainty on behalf of the irrational employee, who might feel betrayed if the employer is using inserted information for devious purposes. The extent to which an employee has such feelings and perceptions should depend on the psychological contract between employee and employer which is described next.

**Psychological Contract Theory**

In an organizational context, the relationship quality between an employee and his or her employer depends greatly on the psychological contract held by the specific employee (e.g., Morrison and Robinson 1997; Rousseau and McLean Parks 1993; Robinson 1996; Rousseau 1989). A psychological contract refers to an employee’s perceptions of what he or she owes to the employer and what the employer owes to the employee (e.g., Morrison and Robinson 1997; Robinson 1996). The psychological contract presents a rather broad concept and obligations perceived in this regard must not be based on formal contracts but can also result from an employee’s subjective perceptions and implicit conclusions (Morrison and Robinson 1997). Obligations in a psychological contract can include a wide range of elements such as a regular pay, and other short-term benefits, but also more social and relational elements such as loyalty, fairness, trust, or support “through sickness and in health” (Rousseau and McLean Parks 1993, p. 12). Note that psychological contracts are perceptual in nature and not necessarily shared by different actors within the organization (Rousseau 1989).

The quality of psychological contracts helps explaining what employees expect from their organizations (and what not). In this regard, breaches of psychological contracts significantly determine employees’ work-related attitudes and behaviors (e.g., Restubog et al. 2013; Robinson 1996; Zhao et al. 2007). A psychological contract breach can be defined as an employee’s “cognition that one’s organization has failed to meet one or more obligations within one’s psychological construct in a manner commensurate with one’s contributions” (Morrison and Robinson 1997, p. 230). In environments with increasing turbulence and uncertainty, trends such as downsizing, restructuring and reliance on temporary workers can all influence psychological contracts (e.g., Morrison and Robinson 1997). Perceptions of violations in this regard decrease trust toward the employer and, as a consequence, reduce employees’ contributions to the organization (Morrison and Robinson 1997; Robinson 1996).

Linking psychological contract and principal–agent theory, we argue that a decrease in trust through violations of psychological contracts will in turn influence an employee’s perceptions that opportunistic behavior by the organization might be more likely. An employee might be uncertain whether information revealed within REIS will be used by the employer to monitor its employees and thus decrease information asymmetry. In contrast, in the presence of a high quality psychological contract, employees should expect that their information is treated respectfully and in mutual interest. As long as an employee trusts that the employer is upholding his side of the psychological contract, he or she might be more willing to provide revealing information within REIS.

**The Nature of Revealing Enterprise Information Systems (REIS)**

As a foundation for our research, it is crucial to clarify our understanding of REIS. In the following section, we will elaborate on the characteristics of REIS to determine whether an IS can be categorized as REIS.

We declare that information systems can be categorized as REIS if they have the following characteristics:

1. Information is actively disclosed by the employee
2. Disclosed information can decrease information asymmetry in favour of the employer
3. System success depends on honest information provision by the employee
The label REIS thus subsumes IS which require their users to make revealing information about themselves available to the organization in order for the system to be successful. We consider information items as revealing if they help drawing conclusions about an employee that might be relevant for his or her employer, such as his or her personal life, expertise, abilities, well-being, attitude, activities, or location during work. According to this, one characteristic of REIS is that information inserted by the employee can be perceived as a potential threat, since the employer might use it for opportunistic purposes. Taking a look at employees’ daily work, several applications can fall under this category. For example, enterprise social networking platforms, wikis, (micro-)blogs, and other knowledge sharing systems or location-based mobile services can make employees perceive that they are revealing information (e.g., their activities or opinions). All of these enterprise information systems are more or less dependent on the willingness of employees to provide correct and honest information (e.g., Denyer et al. 2011; Koch et al. 2013), whereby ‘the willingness of employees to provide correct information’ does not imply that the usage of REIS has to be voluntary. It rather indicates that employees actively have to decide whether to disclose correct and honest information or not. If employees are uncertain about the employers’ intentions, due to information asymmetries between an employee and his or her employer as well as assumed self-interested behaviour of both parties, it is difficult to verify if information provided is actually true and accurate.

REIS can offer many benefits to employees and the organization as a whole as they generate visibility and transparency regarding employees’ knowledge, activities, preferences, and social network connections (Treem and Leonardi 2012). For instance, companies can use “expert finders” or “skill databases” in which their employees are requested to provide their competencies and experiences to enable other employees access to expert knowledge (Mattoo et al. 1999; Yimam-Seid and Kobsa 2003). In a similar vein, wikis offer an easy way for employees to publish information and make work-related knowledge and activities visible to co-workers (Grudin 2006). Moreover, REIS can enable employees and employers to archive information and therefore facilitate an employee’s daily work. For example, conversations can be persisted by engaging in social media, such as recording discussions with video-conferencing tools, instant messaging, or email. Persistence supports the development of a mutual understanding in communicative settings, document outcomes of conversations, and to give others time to fully understand conversations (Treem and Leonardi 2012). In addition, REIS can be used to obtain employees’ opinions through feedback systems (e.g., 360 degree feedback or employee attitude surveys) and offer the possibility to do so anonymously.

These benefits can only be generated if employees are willing to persist revealing information within REIS. On the downside, persisting information in a system could imply reduced information asymmetry and enable opportunistic behaviour on part of the employer (Allen et al. 2007). Today, innovative technologies, databases, and the use of intelligent algorithms for big data analysis are enabling companies to analyse and understand information in a fast and comprehensive way (Stanton and Stam 2003). For example, implementing an expert system as mentioned above requires the willingness of employees to infer personal information about their skills, competencies, or projects. In a context of competitive pressure and the requirement of staff reductions, usage of automatic algorithms might then enable companies to identify expendable workforce (e.g., skills which are not required any longer). Similarly, data collected from employees’ social network usage could enable companies to control the behaviour of their workforce (Brown and Lightfoot 2002; Jackson et al. 2007; Sewell and Barker 2006). Note that these possibilities may not be intended by the organizations at all. The question is whether employees subjectively misjudge their company’s true (or future) intentions in the context of limited rationality, information asymmetries, and uncertainty.

**Conceptual Framework**

In the following section, we present our conceptual framework. The framework centers around the construct PIBV and illustrates antecedents and outcomes, which are important from the perspective of principal-agent and psychological contract theory. At this point, we want to emphasize that the list of antecedents and outcomes should not be seen as being comprehensive. Additional factors, such as individual differences (e.g., techno-insecurity (Tarafdar et al. 2007), computer anxiety, or computer self-efficacy (Thatcher and Perrewé 2002)) might as well have an impact on the employees’ perceived vulnerability when disclosing information. In order to achieve a good understanding of how the employer-employee relationship and related factors have an impact on an employees perceived vulnerability when
using REIS, this research-in-progress focuses on important influencing factors, which are particularly relevant from the perspectives of principal-agent theory and psychological contract theory.

**Perceived Information-Based Vulnerability (PIBV)**

As argued above, the success of REIS depends strongly on the quality of information a user enters into these systems. In turn, we argue that an employee’s choice to make information available which possibly reduces information asymmetries in favor of the employer is affected by the user’s anticipation of opportunistic behavior. Based on principal–agent’s notion of opportunistic behavior (e.g., Eisenhardt 1989; Jensen and Meckling 1976; Pavlou et al. 2007), we define the user’s perception of information-based vulnerability (PIBV) of a system as the extent to which a system evokes an employee’s fear that information entered into the system could be used in an opportunistic manner by the employer.

PIBV presents a perceived system characteristic which reflects a given user’s strength of belief that making information available in the system could backfire—at some point in time. An information system which only requires an employee to enter sales orders might exert a low degree of PIBV as the sales information do not reveal any characteristics or behaviors about the employee. In contrast, an enterprise social networking tool in which a user’s contributions and group discussions are linked to a personalized account could be associated with increased PIBV because it could make transparent the content of the employee’s conversations such as a (lack of) skills, activities, tendencies, work habits, etc.

Overall, PIBV should be context specific and dependent on a particular constellation between employee, employer, and the system itself. Due to context changes, PIBV might also vary over time. For instance, at a given time, a company might be in a stable situation without pressure to save costs; the need for information about employees’ skills and behaviors could be smaller than in a situation in which economic pressure forces companies to reduce costs. In such a changed context, employees might fear that the economic pressure could lead to layoffs. Therefore, an employee might conclude that the company’s need for information about its workforce is higher—implying an increase in PIBV.

**Antecedents of Perceived Information-Based Vulnerability**

The actual cause why employees’ PIBV might increase with regard to a system is due to the principal–agent problem: due to information asymmetry, an employer has incomplete information whether employees are fulfilling their duties and working contracts (Allen et al. 2007). Since information stored within REIS offer the possibility to draw conclusions about workplace behaviors and attitudes, location, or performance, employees could fear that their employer might use this information in an opportunistic manner. Going further, we propose antecedents of PIBV which are a) contingent on the quality of an employee’s psychological contract, and b) depending on the system’s characteristics.

First, we argue that breaches of an employee’s psychological contract, including decrease of trust in the employer as well as perceived fairness (Robinson and Rousseau 1994), should significantly influence his or her PIBV. As PIBV reflects an individual’s anticipation of opportunistic behavior by the employer with regard to information entered into the system, we expect the employee-employer relationship to play a major role for an individual’s PIBV. Based on Morrison and Robinson (1997), we define the breach of the psychological contract as the perceived failure of the employer to meet one or more obligations within one’s psychological construct proportionally to one’s contributions. Ring and van de Ven (1994) underline that those perceptions of failure and resulting fairness decrease with uncertainty about opportunistic behavior in an exchange relationship. For example, if a company is known for poor treatment of its workforce, an employee will have a lower basic expectation of trust, mutuality, and honest behavior (Robinson and Rousseau 1994). Otherwise, if a company has historically adopted principles such as reliability and concern for its staff, employees will have higher expectations for fairness, mirrored in the psychological contract (Morrison and Robinson 1997) and therefore PIBV should be lower. We therefore argue that employees who have felt that their psychological contract was violated will adjust their beliefs accordingly (Restubog et al. 2013). As their trust is significantly impaired by the prior contract breach, they should perceive a higher probability of opportunistic behavior in the future (Deery et al. 2006). For instance, if companies are already making use of surveillance software to monitor their workforce, employees might feel that the moral border to additionally use data from REIS to satisfy their information need might be relatively low.
We will therefore expect users who have experienced a breach of their psychological contract to also report higher values of PIBV.

**P1: A psychological contract breach perceived by a REIS user will increase his or her perceived information-based vulnerability of a system.**

Research investigating information privacy in online consumer settings suggests that the perceived sensitivity of information requested by a system significantly influences the individuals’ decisions to provide personal information items (e.g., Malhotra et al. 2004; Phelps et al. 2000). Perceived sensitivity of information is defined as “a personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent” (Dinev et al. 2013, p. 302). As the principal–agent perspective assumes that the quantity and quality of employee’s personal information is asymmetrically distributed between employer and employee and both parties might act self-interested in order to have an information advantage (Pavlou et al. 2007), employees might withhold sensitive information in order to protect themselves from opportunistic actions and preventing the power shift towards the employer. Therefore, we expect the same to hold true for the disclosure of information within REIS. The more information solicited by a system is perceived as sensitive by the employee, the higher the perceived potential damage if information is used opportunistically by the company. Employees will perceive a potential power shift towards the employer when offering sensitive information. Therefore, higher degrees of perceived information sensitivity should increase the user’s PIBV.

**P2: Higher perceived sensitivity of information required from REIS will increase a user’s perceived information-based vulnerability of a system.**

In addition, information privacy research suggests that perceptions of privacy and the disclosure of personal information are significantly determined by an individual’s perceptions of control retained over their information (e.g., Dinev et al. 2013; Krasnova et al. 2010; Phelps et al. 2000). Perceived privacy control refers to an “individual’s belief in his or her ability to manage and release the dissemination of personal information” (Xu et al. 2011, p. 804). The employee’s fear of potential opportunistic behavior associated with PIBV might not relate to the present situation alone. Rather, the employee could believe that information disclosed within a system could be misinterpreted in the future when taken out of context. Therefore, an employee should feel less vulnerable if he or she retains control over the information being able to modify or delete it at any given point in time. Being able to control the dissemination of provided information offers the possibility for employees to control the power shift towards the employer. Therefore the principal–agent perspective supports the proposition that higher perceptions of control might reduce PIBV.

**P3: Higher perceptions of control over information entered into REIS will decrease a user’s perceived information-based vulnerability of a system.**

**Consequences of Perceived Information-Based Vulnerability**

We argue that a user’s PIBV should be strongly related to outcomes that can characterize the quality of REIS usage. Based on principal–agent theory, psychological contract theory, as well as information privacy research, we argue that three types of outcomes are particularly relevant with regard to REIS: decrease of usage activities, favorable coping, and active resistance.

First, employees’ perceptions that inserting information into REIS might be used for opportunistic actions should cause them to interact accordingly and more cautiously with these systems. As illustrated above, REIS may in many cases depend on user’s contributions of honest content such as feedback, comments, or helpful suggestions. By their nature, employees’ input of quality information into REIS may be hard to enforce and the correctness of information may be hard to verify. Research on B2C contexts such as e-commerce or online social networks has found that users’ fears of opportunistic behaviors will greatly decrease their willingness to provide personal information (e.g., Dinev and Hart 2006; Li et al. 2010; Okazaki et al. 2009; Son and Kim 2008). In an organizational context, research suggests that employees’ honest contributions, extra role behaviors, and behaviors that indicate that they responsibly participate in or are concerned about the life of the company are affected by the quality of psychological contracts (Morrison and Robinson 1997; Robinson 1996; Rousseau 1989). We therefore expect that REIS usage and provision of quality information should strongly depend on a user’s PIBV. In this case, employees might
only use a system to the extent which is necessary but avoid entering honest information which can help improve the work of others or the company as a whole.

**P4:** Higher perceptions of information-based vulnerability of REIS will decrease a user's extent of usage of the system.

As an additional consequence of higher PIBV, employees could engage in favorable coping behaviors. In the presence of information asymmetry, one such coping behavior might be impression management or lying on part of the agent (Eisenhardt 1989). Perceptions that information entered into a system might be visible to managers could therefore lead to increased self-presentation and impression management which involves behaviors directed at creating desired impressions (e.g., Eisenhardt 1989; Gardner and Martinko 1988a). Employees would then exaggerate the information provided in a system which might present themselves more favorably in front of their employers (Gardner and Martinko 1988a, 1988b). Again, due to the nature of REIS, employees can often decide which information to enter in these systems and, due to information asymmetries, others might not be able to fully validate whether this information provided is actually true. This could result in incorrect or imprecise information which would fail the original purpose intended with a system.

**P5:** Higher perceptions of information-based vulnerability of REIS will increase a user’s extent of impression management within the system.

Finally, we propose that—due to its possible relation to psychological contract breaches—higher PIBV could also lead to active or even aggressive resistance such as sabotage, undermining the system’s benefits, or badmouthing (Lapointe and Rivard 2005). Furthermore, as Restubog et al. (2013) point out, employees who feel that their psychological contract was breached might engage in deviant behavior. As research on psychological contract breaches in organizations shows, such violations are often associated with strong emotional reactions such as anger (Morrison and Robinson 1997; Zhao et al. 2007). Overall, employees’ higher PIBV imply that they fear that information might be used against them. IS in general which are perceived as a threat or to shift power away to an opposing party are subject to resistance by its users (Lapointe and Rivard 2005; Markus 1983).

**P6:** Higher perceptions of information-based vulnerability of REIS will increase a user’s active and aggressive resistance towards the system.

In sum, we propose that an employee’s psychological contract quality as well as the possibilities of opportunistic behavior influence the quality of REIS usage. We further propose PIBV as a mediating construct in these relationships as it reflects the mechanisms induced by expectations of opportunistic behavior with regard to a system and thus synthesizes and transfers its antecedents’ effects on its outcomes, Figure 1 shows the summarized research framework.

---

**Figure 1. Research Framework**

---

**Perceived Information-Based Vulnerability of Enterprise Information Systems**
Methodology

At the time of writing, we have already conducted extensive interviews with users of different REIS to assess the relevance of PIBV, gather feedback on the construct itself, as well as its antecedents and outcomes. In the next step, we seek to generate scale items for PIBV based on our field notes which need to be evaluated in terms of their dimensionality and validity (e.g., Churchill Jr 1979; MacKenzie et al. 2011). Having specified the measurement model, we will be able to accompany the introduction of a newly developed REIS within several companies and to collect field data for further scale validation and model testing.

Potential Contribution

We see strong potential in this research to acknowledge the current developments in the field of enterprise information systems. As organizations increasingly adopt innovative technologies for interaction and collaboration while possibilities for fast, creative, and automated data analysis grow, we believe that the success of systems such as REIS will be more and more dependent on the relationship quality between employer and employee. This particular link between relationship quality and REIS success should be crucial as relationships between employees and employers should be difficult to influence short-term. Companies investing in the development and introduction of REIS need to consider this perspective to obtain value from these systems. Our research could present a valuable contribution by pointing toward the peculiarities of REIS success.

References


