Normalizing the Shadows – The Role of Symbolic Models for Individuals’ Shadow IT Usage

Research-in-Progress

Steffi Haag
Goethe University Frankfurt
Grueneburgplatz 1, 60323 Frankfurt
haag@wiwi.uni-frankfurt.de

Andreas Eckhardt
Goethe University Frankfurt
Grueneburgplatz 1, 60323 Frankfurt
eckhardt@wiwi.uni-frankfurt.de

Abstract

Employees increasingly use cloud services of third party providers to efficiently perform their job. Interestingly, the majority adopts the cloud without approval of the organization. IT resources like that are commonly referred to as shadow IT. Although widespread in practice, the present literature on shadow IT is scarce lacking a clear definition of the phenomenon and exclusively focusing on the organizational perspective. This research addresses the issue at the individual level. We define shadow IT usage as voluntary usage of any IT resource violating injunctive IT norms at work as reaction to perceived situational constraints with the intent to enhance work performance, but not to harm the organization. Building furthermore on theories of organizational frustration, social learning, and norm salience, we develop a research model of individuals’ shadow IT usage to analyze the inhibiting effect of explicit IT usage restrictions on users’ deviant behaviors in a future laboratory experiment.

Keywords: Shadow IT, shadow IT usage, injunctive norms, situational constraints, organizational frustration

Introduction

Both information technology (IT) and business line employees increasingly use cloud-based software services provided by third party providers to efficiently perform their job (Stadtmueller 2013). Interestingly, more than 80% of them initiate the software-as-a-service (SaaS) adoption themselves without the approval and thus, against the prevailing IT procedures of the organization, as a recent survey among practitioners shows (Stadtmueller 2013). Those IT resources are commonly referred to as shadow IT and substitute or complement the organizational IT infrastructure centrally managed by the IT department (Behrens 2009; Ortbach et al. 2013; Schalow et al. 2013; Winkler and Brown 2014).

Whereas in the past mainly tech-savvy employees were able to improvise and work around approved information systems (IS) using, for instance self-developed spreadsheets (Alter 2014; Behrens 2009), today emerging business and consumer devices like USB sticks, mobile smartphones, or tablets, and, in particular, on-demand service delivery models in the cloud, promote shadow IT in business and with it, introduce great risks and threats to the organizational IT security (Erbes et al. 2012; Györy et al. 2012; Haag and Eckhardt 2014). Employees might rationalize their self-initiative with improvements in personal and/or organizational performance by compensating for and hinting at potential limitations and inefficiencies of the available enterprise IT systems, rules and procedures; but still their acting represents a serious threat to corporate IT security and a violation of injunctive IT norms (Györy et al. 2012; Scott
and Wagner 2003; Stadtmueller 2013) pre- and/or proscribing what is commonly approved at work (Cialdini et al. 1990, 1991). Hence, the interesting question remains of how can organizations counteract employees’ motivations to use shadow IT?

Although established IS journals increasingly recognize the phenomenon (Alter 2014; Winkler and Brown 2014), the present literature on shadow IT so far is scarce and primarily discusses causes (Behrens and Sedera 2004; Kerr et al. 2007), consequences (Behrens 2009; Jones et al. 2004), or potential governance approaches (Beimborn and Palitza 2013; Györy et al. 2012) from the organizational perspective. While the consequences of the shadow IT usage could be sensed and measured at the organizational level, the actual appearance occurs at the individual level. Interestingly, our literature review could not identify any study that explicitly theorizes and empirically investigates antecedents and consequences of employees’ shadow IT usage at the individual unit of analysis. Consequently, specific motivators of employees’ shadow IT usage and calculated managerial counteractions are more or less uncharted.

Therefore, as a first step to close this gap, this research intends to a) clearly conceptualize and delineate shadow IT usage taking a behavioral, normative perspective (Dodge 1985) and b) develop and empirically evaluate a research model of individual shadow IT usage at the workplace grounded in the theories of organizational frustration (Spector 1978, 1997), social learning (Bandura and Walters 1963; Davis and Luthans 1980; Manz and Sims 1981), and norm salience (Cialdini et al. 1990, 1991; Kallgren et al. 2000). In doing so, we argue that situational constraints regarding insufficient IT systems stimulate the use of unapproved IT to accomplish one’s job, and we examine the influence of salient injunctive IT norms represented by IT usage restrictions on the individuals' response. Hence, our research question is:

What is the impact of IT usage restrictions on employees’ shadow IT usage?

We focus on the normative perspective of individual shadow IT usage, because researchers and practitioners predominantly propose the establishment, adjustment as well as the explicit communication of injunctive IT norms, such as IT usage restrictions, in order to deter user rule-deviant intents (e.g., Bacharach et al. 2002; D’Arcy et al. 2009; Greenberg 2002; Hegarty and Sims 1979; Hovav and D’Arcy 2012; Stadtmueller 2013). By contrast, there is a lack of and call for research considering the actual effect of “the nature of the rule itself” (Morrison 2006, p.23) on its violation. Thus, our findings may offer a theoretical foundation for the making and enforcement process of organizational IT directives and substantiate managerial counteractions regarding shadow IT.

The remainder of this research-in-progress will first draw from literatures on social psychology, organization, management, and IS to delineate the deviant behavior of shadow IT usage and its potential environmental and situational antecedents. Based on this conceptualization as well as theories on organizational frustration (Spector 1978, 1997), social learning (Bandura and Walters 1963; Bandura 1969), and norm salience (Cialdini et al. 1990, 1991), we develop a research model of the individual shadow IT usage and hypothesize the moderating impact of focal IT usage restrictions on the relationship strength between IT-related system constraints and the use of shadow IT. Finally, we outline the research design revolving around our future laboratory experiment.

Research Background

This section reviews the body of knowledge of social norms, organizational frustration, and shadow IT in order to rigorously define the behavior of shadow IT usage adopting a normative approach from sociology (Dodge 1985; Spreitzer and Sonenshein 2004). Afterwards, we justify the theoretical reasoning of our subsequent research model based on key literature on related employee misbehavior in the fields of workplace deviance, business ethics, IS security, and undesired IT usage.

Normative Background of the Shadow IT Concept

Conceptualizing shadow IT usage from a normative perspective and analyzing the impact of an explicitly stated normative instruction on employee behavior necessitates to start with the embedding of the concept in the theoretical background of social norms, social learning and social conformity.

In general, norms sum up the behavior of a referent group. They evolve from actively and/or passively sharing with others survival-related actions, which are contingent on the local environment and culture (Cialdini and Trost 1998; Davis 1969; Sherif 1966). Social norms encompass descriptions of effective
conduct by informing about what is typically done in a given situation (descriptive norms), but also the prescription of desired as well as the proscription of undesired behavior. These injunctive norms enjoin what should be done and specify what group members commonly approve, stated explicitly or not (Cialdini and Trost 1998; Cialdini et al. 1990; Deutsch and Gerard 1955). Thus, they indicate the maximum appropriate behavior within the group and set limits of acceptable deviances along the behavioral continuum. “Too far” divergences in any direction may result in negative sanctions for the deviant. To support social injunctions, expressly specified and actively transmitted laws and guidelines may develop. Therefore, group norms affect performance by regulating and regularizing individuals' judgments concerning the appropriateness of the behavior, especially when faced with uncertainty (Axelrod 1986; Cialdini and Trost 1998; Davis 1969; Feldman 1984; Sherif 1966).

Besides of behavior modifications resulting from environmental consequences (reinforcement; Skinner 1938, 1953, 1969), social learning theory suggests that humans also learn through antecedents, that is, through discriminative stimuli before the behavior occurs (Bandura and Walters 1963; Bandura 1969; Davis and Luthans 1980; Manz and Sims 1981). These behavioral changes stem from observing the behavior of others, i.e. models, and the reinforced consequences. For example, if the model's behavior is sanctioned, the observer may less likely imitate it and hence, the vicarious experience may inhibit its behavior (Manz and Sims 1981). Next to real-life observations, the presentation of symbolic models, for instance through active instructions prescribing the correct sequence of conduct in a very clear and direct way, could shape and passively control individuals’ behavior, though to a lesser extent. Likewise, references to exemplary models reflecting social norms do serve as cues that convey appropriate responses to given stimulus situations. Consequently, normative influences, either descriptive or injunctive, represent specific cases of vicarious learning/modeling (Bandura and Walters 1963; Berg and Bass 1961).

However, the strength of the modeling effect and hence, the degree to which injunctive norms actually guide behavior, is subject to whether or not individuals have integrated the norm into their self-concept (Cialdini and Trost 1998; Staub 1972). Internalized values learned from shared expectations in social interactions form one's personal norms and represent individual's anticipation of self-approval of the own behavior in a specific setting (Cialdini and Trost 1998; Schwartz 1973; Sherif 1966). The activation of personal norms ought to differ with the level of awareness concerning one's personal responsibility and the consequences for others (Cialdini et al. 1991; Schwartz 1973; Staub 1972). Accordingly, the successful neutralization of one's activated personal norm, such as to conform to an injunctive norm, may permit its violation without self-deprecation and thus, the volitional deviation from approved behavior in the group (Schwartz 1973).

Finally, besides of the degree of individual's internalization, the effect of a norm on personnel behavior depends to a great extent on its salience in a given setting (Cialdini et al. 1990, 1991; Kallgren et al. 2000; Staub 1972). In particular, if there is a large amount and possible conflict of general social norms and situational models vying for attention, the specific context may trigger the decisive norm ultimately guiding individuals' perceptions of appropriate behavior. Cialdini and colleagues systematically evaluated this important role of salience in their focus theory of normative conduct (Cialdini et al. 1990, 1991; Kallgren et al. 2000).

According to Eckhardt et al. (2008, 2009), referent groups in IS usage scenarios could be classified in groups of the private, public, and working environment. To account for referent groups in individual's working environment, we follow their suggestion and include relevant authorities and peers at the organizational, departmental and team level. Our research model concentrates on the influence and thus, the internalization and salience, of a specific injunctive norm actively and expressly proscribing the unapproved IT conduct for job accomplishment as symbolic model to transmit and guide employee behavior. To be more precise, we analyze the normative presence of explicit IT usage restrictions, the most severe, and thus, visible forms of IT injunctions to direct individuals’ behavioral reactions to insufficient work situations. The next section explains how such situational constraints might easily lead to employee misbehavior owing to the experience of frustration.

**Organizational Frustration Background of the Shadow IT Concept**

Building on the frustration-aggression-hypothesis of social psychology (Dollard et al. 1939), Spector (1978, 1997) develops and expands a model of how frustration affects individual behavior in the
organization. Accordingly, any environmental event in the immediate work situation that constrains or prevents an employee’s task performance and personal goals can be considered a frustrator and thus, a starting point of the job frustration process. Peters and O’Connor (1980) provide a taxonomy of performance relevant situational variables that serve as examples of potential frustrators. Among others, they highlight specific tools and equipment as well as job-related information from stakeholders or company policies, which are all necessary to do the assigned work. If the individual appraises the situational variable as being a frustrator, s/he will experience frustration, the affective reaction to the constraint. This negative affect might in turn evoke varying behavioral responses depending on individual characteristics and the degree of emotional arousal. Mild frustration, for instance, probably challenges people to devise workarounds to reach their objective.

Subsequent research empirically validated and adapted the model of organizational frustration with personality traits and/or formal controls in the context of counterproductive or deviant workplace behaviors (Fox et al. 2001; Fox and Spector 1999; Lawrence and Robinson 2007). Nevertheless, as far as we know, how explicit injunctive norms might counteract individual’s misbehavioral reaction to the negative affect is still unresolved. We address this issue in our research model by investigating the inhibiting effect of IT usage restrictions on the relationship strength between IT-related system constraints and individuals’ usage of shadow IT. In the next section, we first conceptualize this behavior in a clear and comprehensive manner by complementing our previous theoretical reflections with a review of the research stream on shadow IT.

Conceptualization of Individual Shadow IT Usage

To get an overview of the current body of knowledge and to collect previous definitions of the phenomenon, we conducted a comprehensive literature analysis and queried the search engines of the outlets ranked within the MIS journal rankings1 as well as Google Scholar for the terms “shadow IT” and “shadow system”. Following Webster and Watson (2002), we additionally performed forward- and backward search within the identified articles. In the end, we discovered merely a few studies that explicitly and primarily focus on the topic at hand. While Györy et al. (2012) and Rentrop and Zimmermann (2012) investigate how to effectively approach shadow IT in general from a governance and strategic perspective, the remaining six contributions focus on a specific sub-category: shadow systems after an ERP implementation (Behrens and Sedera 2004; Behrens 2009; Jones et al. 2004; Kerr et al. 2007), user-created groupware for collaboration (Shumarova and Swatman 2008), employees’ private mobile devices (Beimborn and Palitza 2013), and stealth SaaS adoption (Zainuddin 2012). All eight articles are published in conference proceedings (except for Behrens (2009)) and approach the phenomenon at the organizational level.

By contrast, research on users’ shadow IT behavior at the individual unit of analysis was only examined in a broader sense, for instance, within the context of workarounds (Alter 2014) or IT consumerization (Ortbach, Bode, et al. 2013; Ortbach, Koeffer, et al. 2013; Schalow et al. 2013). However, these articles also include approved behavior of IT usage and hence, do not appropriately take into account the significant inherent norm violation of shadow IT users. Furthermore, our review identified that there is a lack of a comprehensive and clear conceptualization of the shadow IT usage, though all studies mentioned above seem at least agree upon the norm deviation characteristic by emphasizing the covert deployment of shadow IT (e.g., Behrens 2009; Zainuddin 2012), the non-approval of the firm (e.g. Beimborn and Palitza 2013), or the circumvention of organizational directives (e.g., Györy et al. 2012; Ortbach et al. 2013).

Building on this understanding as well as the theoretical contemplations outlined above and considering normative discussions about related misbehaviors of individuals in sociology and organization science, this study defines shadow IT usage as the voluntary usage of any IT resource violating injunctive IT norms at the workplace as reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization. Shadow IT usage is voluntary since employees are not mandated, but engage in the IT use by themselves either because they are not motivated to comply with or become motivated to departure from expected, routine or actual IT behavior in the organization

---

Normalizing the Shadows

(1978, 1979; Laczniak and Inderrieden 1987). Shadow IT may encompass the old system, the prescribed in an unintended manner (Alter 2014; Silva and Fulk 2012), or a new one, whether software or hardware, on-premise or on-demand, self-developed or purchased, subject to or free of charge, and whether complementing or substituting the organizational IT infrastructure (Beimborn and Palitzza 2013).

Using shadow IT refers to deviant behavior from prevailing injunctive IT norms summarizing the appropriate use of IT at the workplace and covering, for instance, IT rules, directives, procedures or routines, that is, having under control, the organization and/or proximal peers would approve of its employees and/or colleagues not conducting the behavior (Griffin and Lopez 2005; Györy et al. 2012; Ortbach et al. 2013). Consequently, the usage of shadow IT may point to a gap between injunctive norms and employees’ personal norms regarding the proper IT use for task accomplishment. Situational constraints like the established injunctive IT norms or the current IT systems that are perceived as preventing the individual from achieving a desired goal (Alter 2014; Behrens 2009; Györy et al. 2012; Peters and O’Connor 1980) may trigger and activate the salience of one’s personal norm. The normative predominance of the self might then justify the usage of shadow IT for goal accomplishment. That is why we finally allege that the shadow IT user is primarily interested in the efficient achievement of its work tasks (Silva and Fulk 2012) and, even if not intended, recklessly accepts potential damages with different degrees of severity for the organization (Györy et al. 2012).

That does not exclude that shadow IT usage might also be seen as innovative behavior that is constructive and valuable for the organization (Behrens 2009; Györy et al. 2012; Scott and Wagner 2003). In particular, when the organizational IT systems are malfunctioning or prevailing injunctive IT norms are inefficient, shadow IT could provide new perspectives for the firm and foster internal organizational adaptation to altering environmental conditions based on new technology. Staw and Boettgers (1990) study on counter-role behavior with respect to task revision and research on constructive deviance (e.g., Morrison 2006; Vadera et al. 2013; Warren 2003) or positive resistance (Ferneley and Sobreperez 2006) emphasize similar points. However, whether the positive or the negative organizational consequences of shadow IT usage predominate, that should be beyond individuals’ appraisal procedure. Crucial for this study are employees’ judgments of the adequacy of the available organizational IT systems, instructions, or procedures to efficiently complete their own work tasks.

Note that this study concentrates on shadow IT usage of an individual acting alone and independently. Nevertheless, the behavior and its concept might also be found among workgroups, departments and top managers temporarily or over extended periods (Alter 2014; Behrens 2009; Zainuddin 2012).

**Impact of Explicit Injunctive Norms on Shadow IT Usage**

Theoretical and empirical support for the inhibitory effect of explicitly stated injunctions on shadow IT usage can be found in four research streams on related employee behaviors, in which the norm violating characteristic of the phenomenon plays a crucial role.

First, the management literature may label shadow IT usage as organizational misbehavior or workplace deviance from significant organizational norms, which should primarily benefit the employee and may stand somewhere in between counterproductive and constructive outcomes for the firm and/or the society (Griffin and Lopez 2005; Robinson and Bennett 1995; Vardi and Wiener 1996; Warren 2003). Even if some articles theorize the impact of injunctive norms on workplace deviance (Brief and Motowidlo 1986; Litzky et al. 2006; Martinke et al. 2002; Vardi and Wiener 1996), the majority of empirical studies focuses on descriptive and implicit normative antecedents, such as coworker or supervisor behavior (e.g., Dineen et al. 2006; Dunlop and Lee 2004; Morrison 2006; Robinson and O’Leary-Kelly 1998). By contrast, empirical evidence for explicitly stated norms as symbolic models of correct conduct is scant. Exceptions are investigations by Sims and Keenan (1998) analyzing the impact of both written policies and informal practices on whistleblowing and Bacharach et al. (2002) showing that the lack of strictly specified and consistently enforced organizational alcohol rules fosters employee problem drinking.

Second, since deviant employee behaviors significantly overlap with un-/ethical actions with volitional consequences for others (Jones 1991; Treviño et al. 2006), research on behavioral ethics should also be insightful for studying shadow IT. For example, the laboratory experiments of Hegarty and Sims (1978, 1979), Laczniak and Inderrieden (1987) and Treviño and Youngblood (1990) found that a corporate ethic...
goal, a letter stating the presidential ethical philosophy, and direct or vicarious reward systems reduce unethical decision behavior. Likewise, Greenberg’s (2002) survey about employee theft confirms the deterrent effect of formal organizational ethics programs. Within the IT context the influence of explicit codes of ethics on unformal IT behavior could also be validated (e.g., Harrington 1996; Kreie and Cronan 2000). However, altogether, the empirical findings of the ethics literature regarding the influence of express codes of conduct on unethical actions are mixed and modest (see the reviews of Ford and Richardson 1994; O’Fallon and Butterfield 2005; Treviño et al. 2006).

Third, casting a look at IS security research and the extended taxonomy of IS security threat vectors (Loch et al. 1992; Willison and Warkentin 2013), shadow IT usage is an internal human source of threat to IS security with the volitional, but non-malicious intention to violate the corporate IS security policy. Hence, the extant behavioral literature on IS security, particularly in the area of benevolent noncompliance (e.g., Guo et al. 2011; Siponen and Vance 2010; Vance et al. 2013), may provide useful insights for our study. However, when weighing the results, we should keep at the back of our minds that the functional character of the intentional act is disregarded. Besides of the importance of subjects’ awareness of implicit workgroup norms (Guo et al. 2011) or others’ presence (Vance et al. 2013), our review identified two studies examining concrete and detailed guidelines as symbolic appeals to the proper use of organizational IT resources: both show an indirect significant effect on IT misuse intention, mediated by employees’ perceptions of sanctions (D’Arcy et al. 2009; Hovav and D’Arcy 2012).

Fourth and finally, the emerging literature on the dark side of IT usage describing, for example, the justification of abnormal and unhealthy technology overuse (Turel et al. 2011), might strengthen the theoretical development and contribution of our research. Yet these articles primarily focus on undesired outcomes to the individual itself, such as feelings of exhaustion owing to stressful technological activities (e.g., Maier et al. 2014; Tarafdar et al. 2010). By contrast, we assume that users benefit from the employment of shadow IT themselves and improve the own task performance. Potential negative consequences for others resulting from the shadow IT usage are disregarded, though.

To conclude, even if we could gather some indications of the influence of injunctive norms on employee deviant, unethical, security noncompliant, or overusing behavior, the extant organizational, management, and IS literature on the topic is still modest. In particular, there is a lack of research that analyzes the effectiveness of explicitly stated instructions on employee misbehavior. With the objective to close this gap and answer our research question stated at the outset of the paper, we introduce our research model in the next section.

A Model of Shadow IT Usage

Our review of the literature in social psychology, organization, management, and IS research points at two important starting points for a parsimony, but meaningful model of individual shadow IT usage: first, in reaction to experienced frustration, situational constraints regarding insufficient IT systems can stimulate the use of shadow IT; second, salient symbolic models, like IT usage restrictions, could affect individuals’ response. We develop our exact hypotheses as displayed in Figure 1 in more detail in the following.
**IT System Constraints as Stimulus of Individuals’ Shadow IT Usage**

In our conceptualization we assume employees to use shadow IT with good, constructive intentions to improve or complete their job at work and not to harm the firm. Consequently, we may conclude that the existing IT systems and/or the prevailing injunctive IT norms within the organization are perceived as insufficient and hence, interfering with or constrain to the individual’s task performance. In particular, if these malfunctioning or restricted IT tools are essential for the accomplishment of the job required by managers and thus, prevent important goal achievement, they may be sources of and appraised as frustrators (Peters and O’Connor 1980; Spector 1997). The greater the extent of these system deficiencies, the effort necessary to overcome the deadlock, and the reoccurrence and stability of the obstruction in daily work, the more frustration will be experienced (Martinko et al. 2002; Spector 1997). Above all, if employees are forced to use a specific IT tool that they assess as inadequate to efficiently complete their job and satisfy the expectations, they should react with more negative affect (Seo et al. 2011; Silva and Fulk 2012). Hence, we hypothesize that:

H1: The higher the IT system constraints, the higher the experienced frustration.

Prior research on organizational frustration found that negative affect and emotions can lead to counterproductive work behavior targeting persons or the organization, such as the deliberate disregard of supervisors’ instructions (Diefendorff and Mehta 2007; Fox and Spector 1999; Fox et al. 2001; Neuman and Baron 1998). However, Spector (1978, 1997) emphasizes that the exact behavioral reaction will depend on the level of experienced frustration. In fact, most frustrators are at first motivating to find alternative, unblocked means to the goal and may even enhance task performance by raising response speed or intensity (Spector 1978). In the shadow IT context, we argue that users experiencing frustration will first make repeated attempts to clear the technical hurdles or try alternate approved IT systems in order to get the desired IT output. However, if it does not pay off, the instance of experienced emotional arousal increases and individuals will be more and more motivated to cope with the negative emotional state (Lazarus 1966). Finally, users purposely reach for unapproved shadow IT to get the job done, although in doing so, they violate prevailing injunctive IT norms at the workplace. We therefore hypothesize that

H2: The higher the experienced frustration, the higher the shadow IT usage.

**IT Usage Restrictions as Moderator of the Stimulus-Response-Relation**

Bandura and Walters (1963) collected substantial evidence that emotional arousal, for example caused by stressful environmental situations, can intensify the likelihood and extent of social behavior modifications, and that the cues offered by a model frequently influence the direction of those behavioral changes. They suggest that different degrees of emotional arousal impact the range of potential responses the observer can attend. Modest emotional states, such as mild frustration preceding workarounds (Spector 1978), facilitate vigilance and imitation.

Applying this to our research context, we argue that in states of frustration experiences resulting from restricted IT systems, employee’s response to use shadow IT will be less likely, if there are explicit IT usage restrictions as symbolic negative models in place. In line with social learning theory (Bandura and Walters 1963; Davis and Luthans 1980), employees vicariously learn either from reading or listening to directives of the improper IT usage conduct within the organization. At the same time when the experience of frustration occurs, they recall and reconstruct those as significant transmitted symbols retrospectively as retrieval cues (Keller 1987; Tulving and Osler 1968) and derive guidance of expected IT usage behavior. At the point of the behavioral decision, the explicitly stated IT usage restrictions are more salient than the personal norm and therefore, according to the focus theory of normative conduct (Cialdini et al. 1990, 1991; Kallgren et al. 2000), users find lesser support for the rationalization of shadow IT acts. In analogue support of our reasoning, Lawrence and Robinson (2007) also propose a moderating effect on the frustration-misbehavior relation by means of environmental constraints. Consequently, we hypothesize that

H3: Explicit IT usage restrictions moderate the relationship between experienced frustration and shadow IT usage in a way that if there are explicit IT usage restrictions, the relationship is weaker.
Besides of the hypothesized effects of IT system constraints, frustration, and IT usage restrictions on shadow IT usage, we also consider individual characteristics in our research model since related work in the field of workplace deviance, behavioral ethics, and IS security points to potential significant influences on our findings. We control for individuals’ self-efficacy (e.g. Morrison and Phelps 1999), stage of moral development (e.g. Greenberg 2002), perceived locus of control (e.g. Treviño and Youngblood 1990), risk-taking propensity (e.g. Morrison 2006), proactive personality (e.g. Miceli et al. 2012), the Big Five of personality traits (e.g. Colbert et al. 2004), and Machiavellism (e.g. Hegarty and Sims 1979). The methodological approach to validate our conceptual model is introduced in the following section.

Research Design

We will conduct a laboratory experiment to test our hypotheses in order to have perfect control over users’ actual shadow IT usage. This should be particularly valuable for the study of social undesirable behaviors where empirical data are difficult to collect and respondents’ self-reported measures might be biased (e.g., Griffin and Lopez 2005; Stewart et al. 2009). Furthermore, by manipulating the exogenous variables and assigning participants randomly to the experimental conditions, causal inferences drawn from the results may be stronger (Festinger 1953; Schwenk 1982). To minimize possible distortions regarding artificiality, we developed an as realistic as possible lab setting.

The experiment simulates a file-sharing task frequently occurring in employees’ daily work. Each participant performs the task alone, in an isolated environment of a separated room containing one PC with no Internet access block. We set up a web-based mail system that limits the maximum size of outgoing e-mail attachments to 2MB and which is declared to be appropriate and approved to accomplish the experimental task. The job includes the access to a scientific journal database, the search for and download of two articles, and the subsequent separate transmission of both files varying in sizes to a given e-mail address by using the provided e-mail system. This has to be done within a specific time frame, whose duration our pilot studies indicate to be appropriate. Before starting the task, subjects get a usage demonstration and a manual instruction about how to search the database. Participants will furthermore be motivated to perform well. As one of the files exceeds the maximum file size of 2 MB, the e-mail system is malfunctioning and the job cannot be completed successfully, at least not in an approved way.

Subjects’ behavioral response to the malfunctioning system is the core of our observation. The factors of interest are IT injunctions, which are varied at two levels: implicitly versus explicitly stated IT usage restrictions. The condition with explicit usage directives involves additional instructions to the subjects prior to performing the task. Here, the task formulation clearly specifies that the download of software from the Internet as well as the use of any other hardware like private USB sticks, mobiles or smartphones, any other email client, or other web and cloud services, such as Dropbox, is not allowed. By recording the desktop of the participants while performing the task, we can control for the actual chosen IT tool for task accomplishment. Thus, shadow IT usage is measured behaviorally if subjects use any of the restrictive IT systems. In the end, all participants are asked to fill out an online questionnaire designed to gather information about their demographics, the degree of experienced frustration (Peters et al. 1980), manipulation checks, and control variables.

Moving Forward and Expected Contribution

The next step is the recruitment of participants. Besides of undergraduate and graduate students enrolled in IS courses at our university, we also promote our study among family and friends and post advertisements for the laboratory experiment in local newspapers and regional groups in social networking platforms to get a pool of subjects with diverse skills, knowledge, and abilities.

We expect that the results of our analyses regarding the impact of IT usage restrictions on employees’ deviant shadow IT usage, but also our clear definition of the concept, will provide an initial basis to encourage to further research on the individual shadow IT usage. In particular, organizational field studies should be valuable to confirm representativeness and generalizability of our outcomes (Festinger 1953; Schwenk 1982). Besides of the IS field, we contribute to the current body of knowledge in organizational behavior where the influence of (explicit) injunctive in comparison with descriptive norms is often neglected. Finally, our findings should serve IT and business managers in practice to derive effective formal actions of how to encounter shadow IT, an uncharted but highly prevalent phenomenon.
References


