JUSTIFYING SHADOW IT USAGE

Steffi Haag, Institute of Information Systems, Goethe University Frankfurt, Frankfurt am Main, Germany, haag@wiwi.uni-frankfurt.de

Andreas Eckhardt, German Graduate School of Management and Law (GGS), Heilbronn, Germany, andreas.eckhardt@ggs.de

Abstract

Employees and/or functional managers increasingly adopt and use IT systems and services that the IS management of the organization does neither provide nor approve. To effectively counteract such shadow IT in organizations, the understanding of employees' motivations and drivers is necessary. However, the scant literature on this topic primarily focused on various governance approaches at firm level. With the objective to open the black box of shadow IT usage at the individual unit of analysis, we develop a research model and propose a laboratory experiment to examine users' justifications for violating implicit and explicit IT usage restrictions based on neutralization theory. To be precise, in this research-in-progress, we posit positive associations between shadow IT usage and human tendencies to downplay such kind of rule-breaking behaviors due to necessity, no injury, and injustice. We expect a lower impact of these neutralization effects in the presence of behavioral IT guidelines that explicitly prohibit users to employ exactly those shadow IT systems.

Keywords: Shadow IT, Techniques of neutralization, Rationalization, IT usage restrictions.

1 INTRODUCTION

Information technology (IT) resources adopted and used without the approval of the IT department are increasingly widespread among employees and functional managers in organizations as recent surveys show (Stadtmueller 2013; Walters 2013). In particular, emerging consumer devices like mobile smartphones or cloud services easily delivered via web browsers make so-called shadow IT also accessible for personnel without excessive IT skills and thus, challenge the organizational information systems (IS) management (György et al. 2012; Haag & Eckhardt 2014; Zimmermann & Rentrop 2014). To balance the pros and cons resulting from the innovative potential and individual performance improvements versus the huge threat to the enterprise information security (Erbes et al. 2012; György et al. 2012; Haag & Eckhardt 2014b, 2014c), researchers and practitioners discuss various governance approaches at firm level ranging from total permission, merely specific concessions, to the company-wide banning of shadow IT (e.g., Beimborn & Palitza 2013; György et al. 2012; Stadtmueller 2013).

However, prior to the design of effective managerial measures, it is important to understand the principles and to know the extent of users' shadow IT usage behavior at the individual unit, where the actual appearance of the phenomenon ultimately occurs. Interestingly, in line with Silic and Back (2014), we could hardly identify any study explicitly and empirically investigating antecedents of persons' shadowy act as well as the actual behavior itself. That might be due to the fact that commonly, employee deviance is difficult to observe and hardly admitted in self-reports (e.g., Griffin & Lopez 2005; Stewart et al. 2009). On the contrary, people rather tend to rationalize and refuse to see their misdemeanors (e.g., Harrington 1996; Robinson & Kraatz 1998; Siponen & Vance 2010).

Therefore, in this study, we develop a research model condensing our theoretical considerations and primarily adopt an approach from criminology explaining rule-breaking behavior based on techniques of neutralization (Sykes & Matza 1957). Neutralization theory posits that persons justify their actions violating social norms by pleading rationalizations which minimize feelings of guilt and shame. Existing research proves the great adaptability of those techniques to deviant, non-compliant behavior in the corporate context (e.g., Greenberg 1998; Hollinger 1991; Robinson & Kraatz 1998) as well as the IS field (e.g., Barlow et al. 2013; Ingram & Hinduja 2008; Lim 2002; Siponen et al. 2012; Siponen & Vance 2010). However, some studies also indicate the potential loss of social controls' efficacy in their presence (Robinson & Kraatz 1998; Siponen & Vance 2010). Hence, we aim to contribute to the existing literature in three ways. We intend to answer the call for further empirical, especially experimental (Siponen & Vance 2010), investigations on the effect of neutralization techniques on intentional insider threats to IS security (Willison & Warkentin 2013). Moreover, by comparing this impact in two different contextual situations of explicit versus implicit IT usage regulations, we attempt to advance the literature on neutralization that identified the interaction with context factors in organizational hand to be missing (Harris & Daunt 2011; Maruna & Copes 2005). Last but not least, with our overall approach, we seek to open the black box of individuals' shadow IT usage (Silic & Back 2014) and particularly response to the following research question

RQ: What is the impact of neutralization techniques on individuals' shadow IT usage?

The remainder of this research-in-progress proceeds as follows. In the next section, we review the extant literature on shadow IT and neutralization theory as basis for the subsequent development of our hypotheses in section 3. Section 4 presents our proposed research methodology and design including variables' measurement, the description of the future lab experiment, and planned data analysis. Finally, we discuss the expected implications for future research and policy-based managerial practice.

2 RESEARCH BACKGROUND

2.1 Prior Work on Shadow IT and Construct Definition

Up to now, not many studies have concentrated on the phenomenon of shadow IT (György et al. 2012; Haag & Eckhardt 2014a; Silic & Back 2014; Zimmermann & Rentrop 2014), though its appearance is increasingly appreciated in top-tier IS journals (Alter 2014; Behrens 2009; Winkler & Brown 2014). Identified shadow IT articles explored sources (Behrens & Sedera 2004; Kerr et al. 2007; Zainuddin 2012; Zimmermann & Rentrop 2014), consequences (Behrens 2009; Jones et al. 2004) such as IT risks for the organizational IS security (Silic & Back 2014), or managerial implications for IT governance (Beimborn & Palitza 2013; György et al. 2012) at the corporate or departmental level of analysis.

Individuals' shadow IT usage behavior, however, was hardy the focus of investigations. Haag and Eckhardt (2014a) conceptualize the use of shadow IT as an affective reaction to experienced frustration, which might be suppressed in the presence of prescribing norms as symbolic models. In a broader context, other individual-level studies focus on workarounds (Alter 2014) or IT consumerization (e.g., Ortbach et al. 2013). However, both do not appropriately consider the norm-violating characteristic of the shadowy act. Consequently, the actual shadow IT behavior, its occurrence and extent as well as specific motivators and justifications of employees are more or less unknown (Haag & Eckhardt 2014a; Silic & Back 2014).

Thus, to open the hitherto black box of shadow IT usage from the individual human perspective and to derive effective measures for the organizational IS management, we adopt the definition of the individual 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"* (Haag & Eckhardt 2014a, p. 4) and with it, a summary of prior understandings in theory and practice (e.g., Behrens 2009; Beimborn & Palitza 2013; György et al. 2012; Ortbach et al. 2013; Silva & Fulk 2012; Stadtmueller 2013). This definition alleges that the shadow IT user acts by her/himself with the primary objective of an effective and productive completion of her/his work tasks (Behrens 2009; Haag 2015; Silva & Fulk 2012; Stadtmueller 2013; Zimmermann & Rentrop 2014), which is jeopardized, for instance, due to malfunctioning or inadequate organizational IT systems or instructions (Behrens 2009; Haag & Eckhardt 2014a; Zimmermann & Rentrop 2014). For this intention, she/he carelessly accepts possible security incidents and damages for the organizational IT assets (György et al. 2012; Silic & Back 2014; Stadtmueller 2013). By utilizing a previous, an adapted, or a new system as supplement or substitute for the organizational IT infrastructure (Alter 2014; Beimborn & Palitza 2013; György et al. 2012), she/he deliberately deviates from existing explicit or implicit IT norms including among others IT rules, policies or procedures (Alter 2014; Beimborn & Palitza 2013; György et al. 2012; Haag & Eckhardt 2014a; Haag 2015; Silva & Fulk 2012).

Sykes and Matza (1957) as well as succeeding research (e.g., Klockars 1974; Lim & Teo 2005; Minor 1981) proposed potential justifications that precede and neutralize those normative deviations and thus, enable users to intentionally engage in rule-breaking acts without self-blame or anticipated criticism of referent others. We present these techniques of neutralization as theoretical framework in the following section.

2.2 Prior Work on Neutralization Theory

The theory of neutralization (Sykes & Matza 1957) was firstly introduced to explain juvenile delinquency by indicating human tendencies to rationalize their criminal behaviors a priori with pleas surrounding, for instance, self-defense, necessity, nonage, or forces beyond one's control. Through the use of these so-called 'techniques of neutralization', people convince themselves and others that their deviant actions are justified and thus, suffer less from feelings of guilt and shame. Consequently, the censure and condemnation of referent others in the social environment is "*neutralized, turned back, or*

deflected in advance" (Sykes & Matza 1957, p. 667) and prevailing norms indicating appropriate behavior are repealed. The individual is excused to engage in deviant acts without harming its self-image and reputation.

Based on the applied method to qualify the norms and evaluate the wrongfulness of the deviance, Sykes and Matza (1957) differentiated between five techniques of neutralization: 1) 'the 'denial of injury', 2) 'the condemnation of the condemners', which both will be discussed in detail below, 3) 'the denial of responsibility' describing deviance due to forces outside of the delinquent's control, such as being in bad company, 4) 'the denial of the victim' by transforming the prey into the perpetrator, while the true wrong-doer slips into the role of Robin Hood, and 5) 'the appeal to higher loyalties', in which the culprit sacrifices society's norms and at the same time satisfies, for example, the interests of her/his friends to solve its inherent dilemma. Besides of examining, refining, and expanding the range (for a tabulated overview see Willison and Warkentin (2013)) of the original five techniques of neutralization (e.g., Klockars 1974; Minor 1981), subsequent research also scrutinized Sykes and Matza's (1957) initial assumption about before-the-act rationalizations, rather than their occurrence afterwards (e.g., Cromwell & Thurman 2003; Gruber & Schlegelmilch 2014; Maruna & Copes 2005). Determined to shed light on the mixed results concerning the temporal order between justifications and deviant behavior, Morris and Copes (2012) applied a longitudinal design and find empirical support for the original theory and the precedence of neutralization techniques. They further point out that the past acceptance of those strategies and subsequent engagement in deviance shapes adolescences' future attitudes towards delinquency and thus, may ease the continuation of misbehavior (Morris & Copes 2012).

Building on the findings in criminology, social science scholars successfully transferred the reasoning to the organizational (e.g., Greenberg 1998; Hollinger 1991; Robinson & Kraatz 1998) and the IS context. Referring to the Internet as double-edged sword, Lim (2002) and Lim and Teo (2005) found that employees primarily legitimize the use of the corporate internet for private purposes (cyberloafing) by balancing out good behavior of the past (known as 'metaphor of the ledger' (Klockars 1974)) or by hinting at the likewise deviant behavior of colleagues ('normalization' (Lim & Teo 2005)), respectively. Likewise, the illegal behavior of copying digital media or software could modestly be explained by invoking techniques of neutralization (Hinduja 2007; Ingram & Hinduja 2008; Morris & Higgins 2009; Siponen et al. 2012). Among those, Siponen et al. (2012) investigated which method has the strongest effect on software piracy intention by measuring each technique with a separated construct and found significant positive relations with 'condemn the condemners' and 'appeal to higher loyalties'. Ingram and Hinduja (2008) further clarified that the importance of neutralization varies with the degree of the pirating act. Analyzing IT misuse in general from an ethical perspective, Harrington (1996) showed the direct and moderating impact of the trait 'denial of responsibility' on IT personnel' judgments and intents concerning computer abuse. Those IT employees with high tendencies to deny responsibilities are more affected by corporate codes of ethics.

Finally, in the IS security area, Siponen and Vance (2010) not only stress the high relevance of neutralization on staff's predisposition to violate IT security policies, but also demonstrate how those methods repeal deterrent measures. Building on these findings, Barlow et al. (2013) suggest that the effect strengths of each neutralization facet depends on the IT-based scenario. For example, in their password sharing setting, 'denial of injury' and 'metaphor of the ledger' were found to be insignificant, while 'denial of necessity', a technique added by Minor (1981) representing deviance because of situational inevitable requirements, is especially supportive. Furthermore, management communication intended to reduce end users' justifications of security policy violations was found to be as effective as their cues pointing out possible sanctions.

To sum up, the existing approaches of neutralization techniques in the organizational and IS field imply that neutralization plays a central role regarding employees' deviant behavior. Nevertheless, several questions still remain unanswered. In particular, there is a lack of experimental research concerning actual and concrete IT-based deviance and its association with techniques of neutralization

(Siponen & Vance 2010; Willison & Warkentin 2013) in varying organizational contextual settings (Harris & Daunt 2011; Maruna & Copes 2005). Simultaneously, the norm-violating characteristic of shadow IT defined in prior literature (see section 2.1) suggests that justifications might be relevant antecedents of individuals' shadow IT usage, as well.

In a future study, we address and combine those issues by analyzing participants' justifications to break implicit and explicit IT usage restrictions set up in a lab experiment. While doing so, we particularly concentrate on three neutralization techniques which have been found to be most important in previous IS literature (Barlow et al. 2013; Lim & Teo 2005; Siponen et al. 2012) and which are primarily applicable to our planned experimental shadow IT scenario. Hence, our selection of and focus on specific neutralization techniques is in line with prior research suggesting that the especially relevant techniques depend on the misbehavior under consideration (Barlow et al. 2013; Harris & Daunt 2011; Siponen & Vance 2010; Willison & Warkentin 2013). In the following, each analyzed neutralization technique and the respective hypothesis is presented.

3 HYPOTHESES DEVELOPMENT

In this section, we provide a detailed reasoning why techniques of neutralization, in particular 'defense of necessity', 'denial of injury', as well as 'condemnation of the condemners', should positively influence individuals' shadow IT usage. Additionally, we posit a greater effect in situations of implicit, that is inaccurately specified, IT regulations.

Defense of Necessity. The 'defense of necessity' enables the offender to break rules when they are indispensable and there are no other alternatives (Minor 1981). Widespread examples are white-collar crimes executed to survive in tough business environments in which illegitimate activities are common practice (Minor 1981; Siponen et al. 2012). Transferred to our research setting, users can point out time pressure to complete a task, which is why they were not able to wait for the official IT support to repair or replace current IT deficiencies. Instead, they revert to known alternate systems to complete their job. Györy et al. (2012) and Zimmermann and Rentrop (2014) report unsatisfied business needs and the slow responsiveness to IT requests as sources of shadow IT. Therefore, we hypothesize:

H1: "Defense of necessity" is positively associated with individuals' shadow IT usage.

Denial of Injury. Focusing on the damage resulting from the deviant act and applying the 'denial of injury', culprits minimize the wrongfulness of their actions if no one was actually hurt by them (Sykes & Matza 1957). In their exploratory study, Lim and Teo (2005), for instance, report that some employees do not understand how short-term cyberloafing could injure the company. With respect to our context, staff not sensitized to potential risks the organizational IT assets are put at when non-approved IT is used, may mainly look at the constructive outcomes of the shadow IT usage like perceived improvements in their own work and with it, the firm performance (Behrens 2009; Haag 2015; Zimmermann & Rentrop 2014). Moreover, prior IS literature pointed out to alienating effects and the lack of personalization in human-computer interactions as cause for IT misbehavior (D'Arcy & Herath 2011; Harrington 1996; Loch & Conger 1996). In line with this, the harmful consequences for the impersonal organization ensuing from individuals' shadow IT usage can further be played down and human's conscience will be eased. Hence, we hypothesize:

H2: "Denial of injury" is positively associated with individuals' shadow IT usage.

Condemnation of the Condemners. Rather than qualifying, the culprit scrutinizes the violated norms utilizing the 'condemnation of the condemners' technique (Sykes & Matza 1957). Hence, she/he redirects attention to the persons that are responsible for the establishment and enforcement of the regulation and consequently, disapprove her/his deviant behavior. Just like viewing the police as corrupt and brutal (Sykes & Matza 1957), in the shadow IT setting, users could blame the IT managers for providing unreasonable or inefficient rules or policies about (im)proper IT conduct in the firm. As a consequence, feelings of guilt and shame owing to the employment of shadow IT are suppressed or lost out of focus. Thus, we hypothesize:

H3: "Condemnation of the condemners" is positively associated with individuals' shadow IT usage.

Implicit versus Explicit IT Usage Restrictions. Finally, we argue that in contextual situations, in which the organizational IT norms governing appropriate IT conduct (e.g. detailed IT usage restrictions) are explicitly declared and communicated, users' tendency to rationalize the shadow IT act will be lower compared to in situations of inaccurately specified, implicit rules. Our reasoning is in line with Robinson and Kraatz (1998) who found that in firms with ineffectual codes of conduct, neutralization techniques were more simply cited. Consequently, we expect that the establishment of well-defined and clear guidelines regarding accepted user behaviors may limit individuals' choice of suitable justifications (Lim 2002) and any intended breach of those regulations will evoke a higher level of self-blame that needs to be overcome. In the IT context, Barlow et al. (2013) validate a significant interaction effect of persuasive managerial statements directed to mitigate employees' neutralizations opportunities to violate the information security policy. Therefore, users that exactly know which kind of IT systems and services are allowed to perform the task and which are not, should find lesser support for the a priori rationalization to turn to shadow IT, than if the usage of alternative IT represents a grey zone without specified boundaries. Thus, our last hypothesis is

H4: Explicit IT usage restrictions moderate the relationship between neutralization techniques and individuals' shadow IT usage behavior to the extent that if there are explicit IT usage restrictions, the relationship is weaker.

Figure 1 summarizes our hypotheses in a research model.

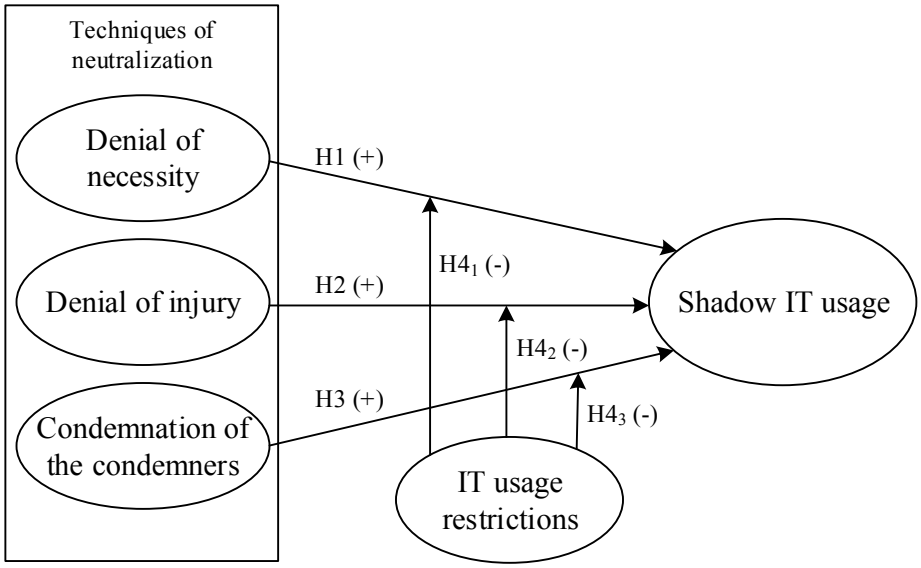

Figure 1. The research model of individuals' shadow IT usage.

4 RESEARCH METHODOLOGY

To test our hypotheses, data collection will take place at three stages, at two points in time (t_1, t_2), and with mixed methods. After identifying potential participants previously registered and endowed with a study-ID, we will first issue a web-based survey to measure attitudinal beliefs of neutralization techniques a priori. Afterwards, we will perform a laboratory experiment allowing us to objectively measure users' actual shadow IT usage behavior. Thus, distortions in our results due to socially desirable responses, a common issue in studies of deviant behaviors (Griffin & Lopez 2005; Harrington 1996; Stewart et al. 2009), may be minimized. For the same purpose, we will always emphasize the anonymity of all participants. The multi-stage approach as well as the choice and pre-test of an as realistic as possible lab setting may further contribute to encountering biases owing to experimental manipulation and artificiality. In addition, we will also include a control group that does

not participate in the pre-experimental survey at t_1 to control for the threat that the arrangement of our initial survey may increase subjects' awareness of neutralization strategies and thus, boost their application and subsequent justifications of shadow IT usage at t_2. We first present variables' measurement and the proposed design of the laboratory scenario at the various stages. In the end of this section, details on the next steps are provided.

4.1 Data Collection at Stage 1

Independent Variables. Several weeks prior to the lab experiment, we will set up a web-based survey including the measures of neutralization techniques. To ensure validity and reliability, three items per neutralization technique are adopted from previous studies (Siponen et al. 2012) and transferred to our research context. On a Likert-scale from 1 ("strongly agree) to 5 ("strongly disagree"), subjects previously registered and endowed with a study-ID will assess statements of rationalizations that are presented in Table 1.

Technique of neutralization	Indicators	Source
Denial of necessity	It is all right to violate rules of conduct and usage under circumstances where it seems like you have little other choice.	Siponen et al. (2012)
	It is acceptable to violate rules of conduct and usage under circumstances where it seems like there is no other option.	
	It is alright to violate rules of conduct and usage if the situation requires you to do so.	
Denial of injury	It is OK to violate rules of conduct and usage if no one gets hurt.	Siponen et al. (2012)
	It is OK to violate rules of conduct and usage if no harm is done.	
	It is OK to violate rules of conduct and usage if no damage is done to the university.	
Condemnation of the condemners	It is not as wrong to violate rules of conduct and usage that seem unfair to you.	Siponen et al. (2012)
	It is not as wrong to violate rules of conduct and usage that seem too restrictive.	
	It is not as wrong to violate rules of conduct and usage that seem unjustified.	

Table 1. Operationalization of techniques of neutralization.

4.2 Data Collection at Stage 2

Lab Experiment. In the experiment, a file-sharing task that may occur in employees' daily work is simulated. For it, we will set up a web-based mail system with a limited maximum size of outgoing email attachments and declare it to be approved and used to accomplish the experimental task in a secure and legitimate manner. In the isolated environment of a separated room containing one PC without Internet access block, each participant will have to send files separately to a given email address within an adequate time frame. Those who successfully complete the task will be allowed to participate in a lottery. At the beginning, subjects will get a usage demonstration and a manual instruction about how to use the database and the provided email system as well as a detailed description of the job procedure. As one of the files will exceed the maximum file size, the email system will fail and the task cannot be accomplishable in the approved way.

Dependent Variable. The focus of our observation will be subjects' behavioral response to the displayed IT system constraint. By recording the PC's desktop while executing the task, we will be able to control for the actual chosen IT tool(s) for task realization. Thus, shadow IT usage will be measured objectively and dichotomously coded if subjects use any other IT systems than those told.

Interaction. To test the moderating effect of explicit IT usage restrictions (H4), we will randomly assign participants to two varying experimental conditions: In the control setting, the restriction is merely implicitly communicated via the strict instruction how to process the job, though without any further cues that convey exact IT exclusions. By contrast, in the treatment setting, the task formulation additionally includes an explicit prohibition to download software from the Internet as well as to use any other hardware like private USB sticks, mobiles or smartphones, any other email client, or other web and cloud services.

4.3 Data Collection at Stage 3

Independent Variables. Subsequent to the experiment, all participants will be asked to again register with their study-ID and fill out a second web-based questionnaire designed to gather information about their demographics, personality, and the post-usage beliefs of neutralization techniques according to the instrumentation in Table 1. The additional ex-post measurement of neutralization will enable us to analyze changes in individuals' beliefs and to recognize potential distortions owing to our experimental setting.

4.4 Moving Forward

Participants. Subjects in the experiment will be undergraduate students who are enrolled in the IS courses at our university and who can gain grade points for participation. Data collection will take place at the beginning (t_1: survey-based study) and in the end (t_2: lab experiment with post-experimental survey) of the term. Only those students who participate in all studies will be included in our future data analysis.

Data Analysis. Here, we will first analyze the records tracking users' reaction to the failure of the mail delivery due to the excess of the maximum possible file size. To test our hypotheses, we will further perform binary logistic regression of neutralization techniques and the interactions with explicit IT usage restrictions on the actual shadow IT usage.

5 EXPECTED CONTRIBUTION

This research-in-progress concentrates on neutralization theory and proposes three kinds of a priori rationalizations that may enhance individuals' shadow IT usage as they do not feel guilt or shame. We expect that our findings will provide initial knowledge on the decision process and the justifications of the individual shadow IT user (Haag & Eckhardt 2014a; Silic & Back 2014), and close the research gaps concerning actual and concrete IS security threatening behavior and its interaction with techniques of neutralization (Siponen & Vance 2010; Willison & Warkentin 2013) in varying organizational contextual settings (Harris & Daunt 2011; Maruna & Copes 2005). Besides of the theoretical contributions, our results may be valuable for IS managers in order to derive measures to encounter new challenges posed by the increasingly emerging trend of employees' shadow IT usage. Positive associations between 'condemnation of the condemners' or 'denial of injury' and shadow IT usage may, for instance, suggest to better communicate and explicate the need to restrict personnel's IT usage. Assessing the effectiveness of changing contextual factors with the establishment of explicit IT usage restrictions, may further provide helpful recommendations for the organizational policy-making and enforcement process. Future research may then extend our findings to include direct and reinforcing effects of perception-based organizational factors, such as employees' fear of expected sanctions owing to their deviance from the IT usage restrictions, on shadow IT usage. It should likewise be valuable to strengthen our findings in a field study, in which, for instance, not only monetary incentives, but also employees preferences for and conveniences of using shadow IT rather than the approved IT can be analyzed.

References

Alter, S. (2014). Theory of Workarounds. *Communications of the Association for Information Systems*, *34*(55), 1041–1066.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*(Part B), 145–159.

Behrens, S. (2009). Shadow systems: The Good, The Bad and The Ugly. *Communications of the ACM*, *52*(2), 124–129. doi:10.1145/1461928.1461960

Behrens, S., & Sedera, W. (2004). Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study. In *Proceedings of the 8th Pacific Asia Conference on Information Systems* (pp. 1713–1726). Shanghai.

Beimborn, D., & Palitza, M. (2013). Enterprise App Stores for Mobile Applications. In *Proceedings of the 19th Americas Conference on Information Systems*. Chicago.

Cromwell, P., & Thurman, Q. (2003). The Devil Made Me Do It: Use of Neutralizations By Shoplifters. *Deviant Behavior*, *24*, 535–550. doi:10.1080/713840271

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. doi:10.1057/ejis.2011.23

Erbes, J., Motahari-Nezhad, H. R., & Graupner, S. (2012). The Future of Enterprise IT in the Cloud. *IEEE Computer Society*, *45*(5), 66–72. doi:10.1109/MC.2012.73

Greenberg, J. (1998). The cognitive geometry of employee theft: negotiating "the line" between taking and stealing. In R. W. Griffin, A. M. O'Leary-Kelly, & J. Collins (Eds.), *Dysfunctional behavior in organizations: Nonviolent behaviors in organizations* (Part B., pp. 147–193). Stamford, CT: JAI Press.

Griffin, R. W., & Lopez, Y. P. (2005). "Bad Behavior" in Organizations: A Review and Typology for Future Research. *Journal of Management*, *31*(6), 988–1005. doi:10.1177/0149206305279942

Gruber, V., & Schlegelmilch, B. B. (2014). How Techniques of Neutralization Legitimize Norm- and Attitude-Inconsistent Consumer Behavior. *Journal of Business Ethics*, *121*, 29–45. doi:10.1007/s10551-013-1667-5

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the Shadows: IT Governance Approaches to User-Driven Innovation. In *Proceedings of the 20th European Conference on Information Systems*. Barcelona.

Haag, S. (2015). Appearance of Dark Clouds? – An Empirical Analysis of Users' Shadow Sourcing of Cloud Services. In *Proceedings of the 12th International Conference on Wirtschaftsinformatik*. Osnabrück.

Haag, S., & Eckhardt, A. (2014a). Normalizing the Shadows – The Role of Symbolic Models for Individuals' Shadow IT Usage. In *Proceedings of the 35th International Conference on Information Systems*. Auckland.

Haag, S., & Eckhardt, A. (2014b). Organizational cloud service adoption: a scientometric and content-based literature analysis. *Journal of Business Economics*, *84*(3), 407–440. doi:10.1007/s11573-014-0716-6

Haag, S., & Eckhardt, A. (2014c). Sensitizing Employees' Corporate IS Security Risk Perception. In *Proceedings of the 35th International Conference on Information Systems*. Auckland.

Harrington, S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly*, *20*(3), 257–278.

Harris, L. C., & Daunt, K. L. (2011). Deviant customer behaviour: A study of techniques of neutralisation. *Journal of Marketing Management*, *27*(7-8), 834–853.

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology*, *9*(3), 187–204. doi:10.1007/s10676-007-9143-5

Hollinger, R. (1991). Neutralizing in the workplace: An empirical analysis of property theft and production deviance. *Deviant Behavior*, *12*(2), 169–202.

Ingram, J. R., & Hinduja, S. (2008). Neutralizing Music Piracy: An Empirical Examination. *Deviant Behavior*, *29*(4), 334–366. doi:10.1080/01639620701588131

Jones, D., Behrens, S., Jamieson, K., & Tansley Elizabeth. (2004). The rise and fall of a shadow system: Lessons for enterprise system implementation. In *Australasian Conference on Information Systems (ACIS)*. Hobart.

Kerr, D. V, Houghton, L., & Burgess, K. (2007). Power relationships that lead to the development of feral systems. *Australasian Journal of Information Systems*, *14*(2), 141–152.

Klockars, D. B. (1974). The professional fence. New York: Free Press.

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, *23*(5), 675–694. doi:10.1002/job.161

Lim, V. K. G., & Teo, T. S. H. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information and Management*, *42*(8), 1081–1093. doi:10.1016/j.im.2004.12.002

Loch, K. D., & Conger, S. (1996). Evaluating Ethical Decision Making and Computer Use. *Communications of the ACM*, *39*(7), 74–83.

Maruna, S., & Copes, H. (2005). What Have We Learned from Five Decades of Neutralization Research? *Crime and Justice*, *32*, 221–320.

Minor, W. W. (1981). Techniques of Neutralization: a Reconceptualization and Empirical Examination. *Journal of Research in Crime and Delinquency*, *18*(2), 295–318. doi:10.1177/002242788101800206

Morris, R. G., & Copes, H. (2012). Exploring the Temporal Dynamics of the Neutralization/Delinquency Relationship. *Criminal Justice Review*, *37*(4), 442–460. doi:10.1177/0734016812456548

Morris, R. G., & Higgins, G. E. (2009). Neutralizing Potential and Self-Reported Digital Piracy: A Multitheoretical Exploration Among College Undergraduates. *Criminal Justice Review*, *34*(2), 173–195. doi:10.1177/0734016808325034

Ortbach, K., Koeffer, S., Bode, M., & Niehaves, B. (2013). Individualization of Information Systems - Analyzing Antecedents of IT Consumerization Behavior. In *Proceedings of the 34th International Conference on Information Systems*. Milan.

Robinson, S. L., & Kraatz, M. S. (1998). Constructing the reality of normative behavior: the use of neutralization strategies by organizational deviants. In R. W. Griffin, A. M. O'Leary-Kelly, & J. Collins (Eds.), *Dysfunctional behavior in organizations: Violent & deviant behavior* (Part A., pp. 203–220). Stamford, CT: JAI Press.

Silic, M., & Back, A. (2014). Shadow IT - A view from behind the curtain. *Computers and Security*, *45*, 274–283. doi:10.1016/j.cose.2014.06.007

Silva, L., & Fulk, H. K. (2012). From disruptions to struggles: Theorizing power in ERP implementation projects. *Information and Organization*, *22*(4), 227–251. doi:10.1016/j.infoandorg.2012.06.001

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, *34*(3), 487–502.

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management*, *49*(7-8), 334–341. doi:10.1016/j.im.2012.06.004

Stadtmueller, L. (2013). The Hidden Truth Behind Shadow IT Six trends impacting your security posture. *Stratecast and Frost & Sullivan; 50 Years of Growth, Innovation and Leadership*. Mountain View, CA. Retrieved April 11, 2014, from http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf

Stewart, S. M., Bing, M. N., Davison, H. K., Woehr, D. J., & McIntyre, M. D. (2009). In the eyes of the beholder: A non-self-report measure of workplace deviance. *The Journal of Applied Psychology*, *94*(1), 207–215. doi:10.1037/a0012605

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*(6), 664–670. doi:10.2307/2089195

Walters, R. (2013). Bringing IT out of the shadows. *Network Security*, *2013*(4), 5–11. doi:10.1016/S1353-4858(13)70049-7

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20.

Winkler, T. J., & Brown, C. V. (2014). Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service. *Journal of Management Information Systems*, *30*(3), 13–47. doi:10.2753/MIS0742-1222300302

Zainuddin, E. (2012). Secretly SaaS-ing: Stealth Adoption of Software-as-a-Service from the Embeddedness Perspective. In *Proceedings of the 33rd International Conference on Information Systems*. Orlando.

Zimmermann, S., & Rentrop, C. (2014). On the Emergence of Shadow IT - A Transaction Cost-Based Approach. In *Proceedings of the 22nd European Conference on Information Systems* (Vol. 73). Tel Aviv.