Dec 10th, 12:00 AM

Empowerment and BYOx: Towards Improved IS Security Compliance

Maximilian v.Welck
University of Augsburg, Faculty of Business and Economics, maximilian.welck@wiwi.uni-augsburg.de

Manuel Trenz
University of Augsburg, manuel.trenz@wiwi.uni-augsburg.de

Tina Blegind Jensen
Copenhagen Business School, blegind@cbs.dk

Daniel Veit
University of Augsburg, veit@wiwi.uni-augsburg.de

Empowerment and BYOx: Towards Improved IS Security Compliance

Short Paper

Maximilian v. Welck
University of Augsburg
Chair of IS and Management
Universitaetsstr. 16
86135 Augsburg, Germany
maximilian.welck@wiwi.uni-augsburg.de

Manuel Trenz
University of Augsburg
Chair of IS and Management
Universitaetsstr. 16
86135 Augsburg, Germany
manuel.trenz@wiwi.uni-augsburg.de

Tina Blegind Jensen
Copenhagen Business School
Department of Digitalization
Howitzvej 60
2000 Frederiksberg, Denmark
blegind@cbs.dk

Daniel Veit
University of Augsburg
Chair of IS and Management
Universitaetsstr. 16
86135 Augsburg, Germany
daniel.veit@wiwi.uni-augsburg.de

Abstract

Non-compliant employees continue to pose a serious threat to information systems security. Most attempts to increase compliant behavior rely on measures that reduce employees' latitude. However, recent studies suggest that this indeed eventuates in less compliance due to adverse behaviors of frustrated or stressed employees. In this study, we propose a novel approach where increased latitude –by means of permitting BYOx– increases the intention to comply. In order to do so, we first construct a theoretical model that links BYOx with empowerment and abuse intention. Subsequently, we run a feasibility study to assess our experimental design and the general feasibility of our propositions. The results suggest that psychological empowerment can indeed be manipulated with vignettes, and that changes in empowerment influence individuals' abuse intentions. Based on such initial promising results, we outline how this novel approach to improve IS security compliance can be developed and investigated further.

Keywords: Information Systems Security, Compliance, Empowerment, IT Consumerization, Shadow IT, Bring your own x (BYOx), BYOD, BYOS, Factorial Survey

Introduction

The damages and costs entailed by digital information security breaches remain a serious problem to the society at large (Aguilar 2015; Coleman 2015). Most often, security attacks originate in breaches of information security policies (ISPs; herein after also referred to as security policies or solely policies) by organizational insiders (Balozian 2016; Burg and Waterfall 2016). Such breaches may appear as the result of strong emotions such as frustration or rage (and hence the abuse is an end in itself), also known as *expressive abuse* (Willison and Warkentin 2013). Alternatively, they may merely be a reflection of

convenience, such as the use of (prohibited) online services to save the time of installing software following cumbersome routines (and hence the abuse is a means to an end). The latter, also known as *instrumental abuse*, is the focus of this study. Instrumental abuse is often referred to as 'shadow IT', 'IT consumerization', or 'Bring Your Own x' (BYOx). BYOx is an umbrella term encompassing Bring Your Own Device (BYOD), Bring Your Own Service (BYOS), etc.

A growing trend in organizations is shadow IT, which refers to IT that is employed behind company firewalls, but remains out of the central IT department's control (Potter and Buchanan 2016). The same definition fits with BYOx, which represents the vastly available online services such as data storages, office-suites (e.g., PDF creators or spreadsheet software), e-mail providers, etc. Such services are also encompassed by the term IT consumerization, which is the phenomenon that consumer technologies (e.g., Dropbox) are being employed for business purposes (Harris et al. 2012). We consider all three phenomena to be synonymous, but confine ourselves to the use of BYOx and IT consumerization.

At present, most attempts to handle IT consumerization, and to increase and understand policy compliant behavior, translate into fear appeal and general deterrence (Lebek et al. 2014). However, the results of these studies are inconsistent (Paternoster 1987; Pratt and Cullen 2005; Siponen and Vance 2010; Willison et al. 2016; Willison and Warkentin 2013). Indeed, already 30 years ago, Paternoster wrote that "*Perceptual deterrence researchers [...] should also begin to prepare themselves for possible bad news. No matter how sophisticated the study or how valiant the effort, very little relationship may exist between people's estimates of the certainty and severity of punishment and their behavior*" (Paternoster 1987, p. 214). What is more, recent studies on the organizational level suggest that intensified information security measures may actually turn out to threaten security; e.g., through adverse behaviors by employees who are stressed or frustrated due to stricter security measures (Balozian 2016; D'Arcy et al. 2014).

Until recently, management sciences, just like information systems (IS) compliance research today, relied on (tight) controls, rewards, punishments, and expected employees to simply comply with work tasks, which only communicated instrumental value (Balozian 2016; Lebek et al. 2014; Thomas and Velthouse 1990). Yet, fiercer business competition in the 1990s, which necessitated employees to have (higher) intrinsic task motivation, paved the way for emphasizing the notion of *empowerment* in management sciences (Ahearne et al. 2005; Thomas and Velthouse 1990). Similarly, today, enterprise solutions compete with powerful consumer IT. Simply prohibiting the use of these technologies by means of information security policies and deterrence is, as outlined above, likely to lead to policy abuses. Yet, preventing their use technically is prohibitively expensive for most SMEs. Thus, we suggest the use of empowerment theory, as an alternative, to motivate employees to comply with information security policies and to prevent the misuse of IT consumerization.

In brief, empowerment is a management concept, aiming at nurturing internalized motivation and commitment by conveying a sense of meaningfulness, participation, confidence, and autonomy (Thomas and Velthouse 1990). In other words, values that are inherently conveyed with the right to use BYOx. Both relationships – BYOx and empowerment – as well as empowerment and behavioral intention to instrumental information security policy (herein after referred to as security policy, or simply policy) abuse – have received little research attention thus far. Consequently, the present study has two aims. The first aim is to advance the understanding of *(I) if and how BYOx shapes empowerment*, and *(II) if and how empowerment influences behavioral intention to policy abuse*. We address this research focus by assessing how empowering leadership (i.e. employees have the right to use BYOx) differs from non-empowering leadership (i.e. employees lack the right to use BYOx) in shaping normative judgements on intention to abuse policies. The second aim of this study is a feasibility check, as it is not self-evident that the aforementioned theoretical aims are empirically testable.

The paper is structured as follows. First, we present the theoretical background and develop our research hypotheses. Second, we present the empirical methodology together with the construct measurements. Finally, we conclude by discussing the results of the feasibility check and the anticipated future research outcome.

Theoretical Framework

In line with our research focus, and as depicted in the conceptual research model in Figure 1, we assess the influence of BYOx on psychological empowerment (Conger and Kanungo 1988; Thomas and Velthouse

1990), as well as the influence of psychological empowerment on behavioral intention to instrumental policy abuse. (BYOx is merely an aggregated 'Bring Your Own' level, which includes multiple similar yet distinct Bring Your Own designs.) The behavioral intention is seen as an indicator of a predisposition to commit a policy abuse, not as a direct proxy for actual behavior (Paternoster and Simpson 1996).

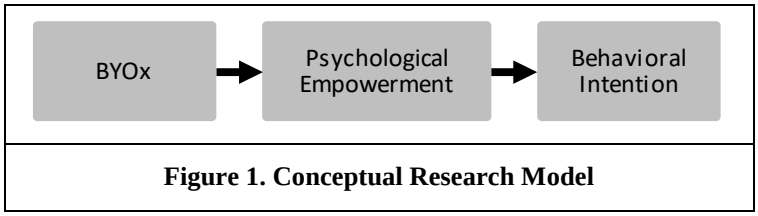

Figure 1. Conceptual Research Model

We base this initial understanding on recent work by Willison et al. (2016), Zhang and Bartol (2010), and Rossi and Nock (1982), as described next.

Empowerment Leadership and Psychological Empowerment

Empowerment represents the sharing of power with subordinates to encourage more initiative and persistence (Thomas and Velthouse 1990). Power here refers to *authorizing* (legal), *energizing* (energy), and *self-efficacy raising* (capacity) (Thomas and Velthouse 1990). Conger and Kanungo (1988) differentiate between 'empowering leadership', which represents a relational construct, and 'psychological empowerment', which is a motivational construct. This contentual differentiation is important since empowering leadership, limited to the delegation of power and responsibility, may leave the employee feeling overburdened (Maruping and Magni 2012) or, to the contrary, overconfident (Conger and Kanungo 1988), but without any perception of being more psychologically empowered. Thus, although a close, and positively tested, relationship between both constructs exists, the former merely paves the way for the latter, but cannot necessitate it (Ahearne et al. 2005; Conger and Kanungo 1988; Kirkman and Rosen 1999; Seibert et al. 2004; Spreitzer 1995; Thomas and Velthouse 1990; Zhang and Bartol 2010).

To encourage the perception of psychological empowerment, Conger and Kanungo (1988) suggest an empowering leadership style, which consists of four leadership practices. These practices include: (A) setting of inspirational and **meaningful** goals; (B) allowing employees to **participate**; (C) expressing **confidence** in employees; and (D) providing **autonomy** from bureaucratic constraints in such a way that employees receive just enough guidance to not feel left alone (Randolph 1995).

With the clarification of empowerment, we move on to discussing empowerment leadership. We take our point of departure in IT consumerization for two primary reasons. First, employees are met with a tremendous breadth of possibilities to make use of BYOx which has become a growing concern to organizations (Potter and Buchanan 2016). Second, three of the four leadership practices leading to psychological empowerment are inherent in being allowed to make use of IT consumerization – only meaningful goals (A) are not necessarily immanent to this right. This is a circumstance that is likely to reduce, but will not fully offset, the perception of empowerment leadership and psychological empowerment (Spreitzer 1995). The remaining three leadership practices are immanent to the right to use BYOx: participation (B) derives from the fact that with BYOx it is the employee, or a group of employees, who decides over which means of work and communication to make use of, instead of the central IT department. Further, the right to use BYOx is an expression of confidence (C): The Meriam Webster and the Cambridge online dictionary depict 'confidence' as the *"faith or belief that one will act in a right, proper, or effective way"*, and as "*[…] having trust in people […]*" respectively. BYOx is just that: showing the trust in people that they will act in an effective way, or in other words, expressing confidence. Finally, IT consumerization increases the latitude of employees by reducing the amount of procedures before certain wanted/needed digital online services may be used by the employee; it thus provides autonomy from the bureaucratic constraints (D) brought about by security policies.

For this study, we consider employees who have the right to self-responsibly decide over the use of BYOx, as employees who are exposed to an empowering leadership style. Vice versa, employees who lack this right, are considered to be exposed to non-empowering leadership. The relationship between perception of empowering leadership and perceived psychological empowerment is salient conceptually. Specifically, this relationship has been positively tested in a non-digital environment by Zhang and Bartol (2010).

Psychological empowerment is, as empowerment leadership, comprised of four subdimensions: meaningfulness, impact, competence and self-determination. We will discuss these dimensions in-depth in the next subsection, for easier intelligibility we remain at this point with stating the hypotheses:

H1a: Non-empowering leadership does not affect perceived meaningfulness.
H1b: Non-empowering leadership does not affect perceived impact.
H1c: Non-empowering leadership does not affect perceived competence.
H1d: Non-empowering leadership does not affect perceived self-determination.

H2a: Empowering leadership positively affects perceived meaningfulness.
H2b: Empowering leadership positively affects perceived impact.
H2c: Empowering leadership positively affects perceived competence.
H2d: Empowering leadership positively affects perceived self-determination.

Psychological Empowerment and Intention to Instrumental Abuse

As previously argued, the recognition of empowering leadership practices positively affects the perception of psychological empowerment. In accordance with the literature, we define psychological empowerment as a psychological state, which is based on the situational judgement along four dimensions: (1) **meaningfulness**, (2) **impact**, (3) **competence**, and (4) **self-determination** (sometimes also referred to as choice) (Seibert et al. 2004; Spreitzer 1995; Thomas and Velthouse 1990; Zhang and Bartol 2010). (1) Meaningfulness refers to the evaluation of a certain task based on the individual's own ideals and standards (i.e., the intrinsic devotion to the task). (2) Impact refers to the individual's evaluation of whether his/her behavior can contribute to the accomplishment of a task. (3) Competence, which is similar to Bandura's (1977) self-efficacy, is the individual's evaluation of whether he/she possesses the necessary skills to achieve a certain task. (4) Self-determination, coined by Deci and Ryan (1985), is the evaluation of the causal responsibility for an individual's actions (Seibert et al. 2004; Spreitzer 1995; Thomas and Velthouse 1990; Zhang and Bartol 2010).

Before continuing with a more detailed description of these four situational judgements, along with a brief discussion of behavioral effects and their influences on intention to behave, we need to discuss briefly the objective of security policies. Security policies serve as a means to reduce the likelihood of adverse events. In other words, the aim of security is the absence of adverse events. Thus, to go one-step further, at the easily perceivable cost of efficiency, an imperceptible outcome is aimed for. Concerning information systems security, a further difficulty arises from the fact that digital threats are especially intangible. This is aggravated by the fact that even damages are often undetectable for non-IT specialists and remain undetected for partially long periods (Ponemon 2016). In essence, from an employee's perspective, the outcome aimed for is imperceptible, threats are intangible, and even actual damages may remain unnoticed; yet, the costs (e.g., reduced efficiency) are evident and immediately perceptible. Having singled out the objective of security policies, we now return to the discussion of the four cognitive judgements.

Giving employees the perception that they can make an impact (2) means that they can effectively contribute to a given task; effectively, in this case, relates to the existence of restrictions imposed by the surrounding circumstances such as security policies. The perception of being effective leads to an increase of all three; emotional stability, motivation, and the ability to recognize opportunities (Thomas and Velthouse 1990). Thus, employees are emotional apt and capable of dealing with (the remaining) constraints caused by security policies. Together with elevated motivation, these facilitate employees with keeping their minds open to opportunities that will allow them to efficiently follow through with their work tasks in compliance with the policies, instead of focusing on the constraints caused by security policies and possibilities to breach these. Thus, we hypothesize:

H3: Higher levels of perceived impact will lead to reduced intentions to instrumental ISP abuse.

If an employee feels to be competent (3), it means that the individual conceives to possess the necessary skills to accomplish certain desired ends. Employees who constantly believe that they lack the necessary skills to perform their work-tasks (e.g., because they have to use complex and non-intuitive digital tools) may lack persistence, initiative, and self-esteem. All three lead to reduced efforts to acquire necessary unknown skills, may diminish the perceived value of security policies, and thus reduce the hesitation to abuse these. The opposite is true for perceived competence, which leads to increased persistence, effort, and initiative (Bandura 1977; Thomas and Velthouse 1990). Thus, we hypothesize:

H4: Higher levels of perceived competence will lead to reduced intentions to instrumental ISP abuse.

Information security policies entail a limitation of latitude. If this limitation reaches a level, which leaves employees with the perception of not having any room left for self-determined (4) choices, it may lead to tension and reduced self-esteem. This, in turn, may lead to a reduced appreciation of security policies, which reduces the reservations regarding breaching information security policies. On the contrary, the perception of self-determination; i.e., the perception of being able to make self-determined choices, leads to intrinsic motivation, flexibility, initiative, resilience, and self-regulation. We have not previously discussed the potential influence of resilience and self-regulation on the intention to instrumental policy abuse; indeed, self-regulation is the ability to refrain from just following one's desires. In a working environment, these desires would result in policy abuses whenever policies noticeably reduce efficiency. Resilience strengthens self-regulation (Deci and Ryan 1985; Thomas and Velthouse 1990). Thus, we hypothesize:

H5: Higher levels of perceived self-determination will lead to reduced intentions to instrumental ISP abuse.

BYOx, as a leadership style, does not per se entail inspirational and meaningful goals (1). Yet, it is not foreclosed that employees will perceive meaningfulness due to BYOx. For example, Junglas et al. (2014) found a positive relationship between BYOx and meaningfulness (in an IS study not related to security). That is why we include the discussion of its effects on intention to instrumental abuse. Perceived meaningfulness results in more commitment and involvement (Thomas and Velthouse 1990). In and of itself, both of these behavioral patterns will improve the opinion on the necessity of security policies, which appreciates the value of compliant behavior while the value of an instrumental policy abuse is discounted. Thus, we hypothesize:

H6: Higher levels of perceived digital meaningfulness will lead to reduced intentions to instrumental ISP abuse.

Having presented the theoretical background along with the research hypotheses, we now turn to describing the methodology together with the construct measurements.

Methodology of the Feasibility Study

Assessment of Normative Judgements

This study aims at investigating if and how BYOx shapes psychological empowerment, and if and how psychological empowerment influences behavioral intention to instrumental information security policy abuse. Consequently, we are interested in individuals' normative judgements (i.e., how something ought to be (Jasso 2006; Wallander 2009)) on intention to instrumental policy abuse, and how these normative judgements are changed through the perception of psychological empowerment. We consider intention as an indicator of a predisposition to commit a policy abuse, but not as a direct proxy for an actual behavior (Paternoster and Simpson 1996). We will argue in the end of this paper that the suitable method to analyze these matters is the factorial survey as formalized by Rossi and Nock (1982); yet, for this short paper, we remain with the feasibility study to assess two issues. First, we are interested in determining the extent to which psychological empowerment can be measured and manipulated based on leadership scenarios in the third person. Second, we want to determine whether the manipulation of empowerment in terms of self-determination and impact influences individuals' intention to abuse.

Before detailing the feasibility check, it is important to clarify how people form judgements. Prima facie, it seems to be (prohibitively) complex to make psychological empowerment tangible to the experimental subject through scenarios. Here we follow Rossi and Nock (1982), who assume that individuals' judgements are structured. This argumentation is based on three observations: First, individuals pay attention to only a relatively small number of seemingly relevant characteristics when making judgements. Smartphones, for example, differ with respect to many obvious and hidden features; yet, a buying decision is based on judgements on just a few of these features. Second, individuals are subject to social consensus; i.e., a group of individuals mostly agrees on which features should be relevant and how to weigh these (e.g., display size of smartphones generally outweighs device weight). Third, individuals are largely consistent in their own judgements, even in the case where they depart from social consensus; e.g., one individual puts more (or

less) weight on display size than the individual's peer group (Rossi and Nock 1982). Consequently, we conclude that it is possible to make psychological empowerment tangible to experimental subjects through vignettes.

Vignettes

Experiments, operationalized through vignettes in a survey, have been employed to study similar problems, although not very often. We refer to two IS studies as precedent-setting: One study by Jarvenpaa and Staples (2001) asks the subject, based on a fictive vignette written in the third person, for the likelihood that he or she would feel that certain knowledge, which was mentioned in the vignette, belongs to him/her and the likelihood of sharing it. A second study by Chaterjee et al. (2015) uses vignettes that are written in the first person (e.g., *"A possibility strikes you. Since you know the password to the professor's website, you can log in to his website […], and actually increase your grades substantially. […]"*). They then ask for items like *"All things considered, it is likely that I might carry out this action in the future?"*

Designing vignettes, which are realistic and common, which are worded as similar as possible, while conveying totally different perceptions of empowerment to the experimental subject, which adhere to the requirements of experiments, and which circumvent the desire of experimental subjects to provide answers which seem to him/her to be socially desirable (social desirability bias), is a delicate task. (Which is why this feasibility study is imperative.) The designing of the vignettes is based on Wallander (2009), Rossi and Nock (1982), Siponen and Vance (2010), and Jasso (2006).

To facilitate the access to how this empirical study was conducted we hereinafter present excerpts from the employed vignettes. The explanation of the policy abuse itself remains identical for both scenarios, and reads as follows: *"One morning, Tom gets a phone call from his colleague Frank who needs help. Frank is currently somewhere outside on his way to meet a potentially large customer for brunch. Frank just wanted to go through his presentation one last time, when he noticed that he can't connect to the headquarters, where it is saved. The presentation contains a number of very sensitive financial figures pertaining the company and some detailed descriptions of a new product which they are about to launch. This information may not be saved on mobile devices (such as laptops), nor in the cloud (such as Dropbox, etc.). Still Frank wants to have this presentation for the upcoming meeting. Thus, he asks Tom to send it to him with SecTrans (which is an online service to transfer big files through the Internet). Tom has never heard of it, still he agrees […]".*

The two workplace scenarios, which convey the empowerment/non-empowerment leadership perception are rather lengthy; hence, we contrast only the most expressive bits of each scenario of our between-subjects design. We start with quoting from the empowerment scenario: *"Susan is an empowering leader: She always explains to Tom and the team how their daily work objectives are important to the overall effectiveness of the company […] This holds for the digital work environment, which is governed by the principle to trust the competencies and integrity of employees […] Still, some essential and important rules are in place […]: This concept says that any new digital item (be it a software program, […], or an online service) has to be considered as harmful until the employee is convinced that the item is indeed harmless – only then it may be employed"*.

The subsequent quotation derives from the non-empowerment scenario: *"Susan is a micro manager: She never explains to Tom and the team how their daily work objectives could be important to the overall effectiveness of the company […] This holds for the digital work environment, which is governed by the principle that employees lack the needed competencies and integrity […] Consequently, quite a number of rules are in place. New digital items (be it a software program […] or an online service) are banned until approved by the IT department […]"*. As stated before, subjects receive either of these two (non-/) empowerment scenarios together with the identical policy violation scenario. Thus, whereas the empowerment environment changes, the abusive act remains the same.

Sample and Construct Measurement

We selected Amazon Mechanical Turk (MTurk) for this feasibility study. MTurk is a crowdsourcing platform where micro tasks can be published to around 400.000 registered users, who will process these tasks for a monetary reward. Typical tasks are fairly simple like audio transcription or document categorization (Deng et al. 2016). Our survey was completed by 51 individual respondents. In the feasibility study presented in

this short paper, individuals were randomly assigned to either the empowerment scenario or the non-empowerment scenario. We then assess the influence of empowerment leadership on psychological empowerment and on the intention to instrumental information security policy abuse. After excluding responses with obvious flaws (e.g., wrongly answered content questions, too short answering times, etc.) we used 41 respondents for the feasibility check.

Regarding the measurement, the items for empowerment leadership were taken from Zhang and Bartol (2010), who draw on the study by Ahearne et al. (2005). It consists of four first-order factors: meaningfulness of work, fostering participation in decision making, expressing confidence in high performance, and providing autonomy from bureaucratic constraints (plus one second-order factor). We had to slightly adapt the items from the first person to the third person; e.g., from *'My manager makes many decisions together with me'* to *'Susan makes many decisions together with Tom'* to fit this study. All items are measured with 7-point Likert scales.

The items for psychological empowerment were drawn from Spreitzer (1995). This construct consists of four first-order factors as well: meaning, competence, self-determination, and impact (plus one second-order factor). As for the previous empowerment leadership dimension, we had to slightly adopt the items; e.g., from *'The work I do is very important to me*' to '*The work Tom does is very important to him*' to fit this study. All items are measured with 7-point Likert scales.

The dependent variable, i.e., intention to instrumental policy abuse, was measured based on a separate vignette (as mentioned previously) that delineated an employee who, in breach of security policies, uses an online service. Four items were used for measurement. The first was drawn from Paternoster and Simpson (1996) and Siponen and Vance (2010). We adopted the response scale from the original 11-point scale (0% to 100%) to a 7-point Likert scale in order to align this response scale with the remaining ones. Further, as single items are always peculiar, we added two intention-related items from D'Arcy et al. (2009), which are also measured with a 7-point Likert scale.

Finally, we controlled for the following five demographic variables: age, gender, work experience, education, and scenario realism measured based on two items, one drawn from Barlow et al. (2013) and the other one drawn from Johnston et al. (2016). Furthermore, we controlled for the subject's current perception of empowerment (drawn from Ahearne et al. 2005) at his/her work place, and for the subject's intention to comply with the security policies at his/her work (drawn from Bulgurcu et al. 2010). All items, for scenario realism, the current perception of empowerment at the workplace and for the subject's intention to comply with the security policies at his/her work were measured on 7-point Likert scales.

Discussion, Anticipated Contributions, and Outlook

Discussion

Our research aims to explore the opposite of most of the current information systems security research endeavors. While a majority of existing research focuses on how the introduction of certain security measures influences the intention to behave, we explore how the empowerment of employees, which in many respects equals the reduction of security measures, influences their intention to instrumentally abuse information systems security policies.

Yet, before we can proceed with our main study, we need to assess if it is feasible in the first place. Thus, we conducted this assessment based on univariate analyses of variance (ANOVA) with the dummy variable 'scenario' (with 1 for the empowerment scenario and 2 for the non-empowerment scenario) as the dependent variable. This results in significant differences for two psychological empowerment judgements: 'self-determination' ($F = 12.111$; $p = 0.002$), and 'impact' ($F = 15.177$; $p = 0.001$). These results indicate that the two different empowerment leadership scenarios indeed convey a perception of psychological empowerment. 'Meaning' ($F = 0.045$; $p = 0.834$) is, as anticipated, not significantly influenced by BYOx. 'Competence' ($F = 0.044$; $p = 0.839$) is, unexpectedly, not significantly influenced by the two scenarios. We interpret these results as follows. First, and most importantly, it is possible to convey the perception of psychological empowerment through vignettes depicting different leadership styles. Second, the vignettes still need to be further rephrased to convey the feeling of competence/non-competence. In a second step, we also assessed whether the manipulation of empowerment in terms of self-determination and impact has an influence on individuals' intention to abuse. There was a significant negative effect of the empowerment

scenario on the intention to abuse ($F = 3.854$; $p = 0.047$). This gives an indication that we could be on a promising path with our research endeavor and that it is worthwhile exploring the relationships between empowerment and IS security compliance further.

Anticipated Contribution

Once we have reliably weathered this initial step, which today seems achievable, we anticipate upon completion of the full study that this research will make a number of distinct contributions to IS security research.

First, our study will eventually contribute to the information systems security, BYOx, and empowerment literatures. This will be achieved by examining psychological empowerment as a mediating mechanism, through which empowering leadership ultimately influences employees' intention to instrumentally abuse information security policies. In this study, empowerment leadership is contextualized based on different governance paradigms concerning the use of BYOx (from permitted to prohibited). As stated beforehand, the assessment of BYOx is relevant due to its widespread and easy availability for employees, and the difficulties and costs associated with its prevention. The 'Bring Your Own' phenomenon has been assessed in the IS security context in its different designs (e.g. BYOD, BYOS) from multiple angles; e.g., nudging through the framing of BYOD security policies (Garza and Guo 2015); security education and awareness programs (Harris et al. 2013; Putri and Hovav 2014); tightness of IT regulations (Györy et al. 2012); fear appeals (Tu and Yuan 2015); and IT staff flexibility (Thomson 2012). Yet, to the best of our knowledge, it has never been assessed together with empowerment to better understand information security abuse intentions. Empowerment is, compared to the 'Bring Your Own' phenomenon, not as new to the research field of IS. Still, it has hardly been employed to assess information security policy abuse intention. For example, Abdul Talib and Dhillon (2015) found a positive relationship between information security compliance intention and empowerment, a finding which is supported by Lee et al. (2016). Nonetheless, besides other distinctions with the present study, both papers do not incorporate BYOx, which we consider to be essential.

Our second contribution is the clarification of the connections between the governance of BYOx, empowerment, and information security policy abuse intention. By this means, we will produce a comprehensive and tested conceptual model that uniquely integrates BYOx with empowerment theory and information systems security theory. We explained the theoretical connections between each of these concepts and concluded that empirical tests confirmed the connection between empowerment leadership, psychological empowerment, and abuse intention (Abdul Talib and Dhillon 2015; Lee et al. 2016; Spreitzer 1995; Thomas and Velthouse 1990; Zhang and Bartol 2010). What remains to be thoroughly assessed is whether these connections hold and whether these connections can be manipulated through permitting/preventing BYOx. Yet, as we have argued, there are strong theoretical reasons to expect BYOx and empowering leadership to be well-positioned to influence fundamentals underlying the intention to instrumentally abuse IS security policies, which is also backed by our preliminary empirical results.

Our theoretical contribution will also present important implications for managers. It is our aim to provide an exit to the currently much researched security "paradox" that leaves managers puzzled about how to motivate compliant behavior without triggering undesirable side effects. On the one hand, particular (latitude limiting) security measures seem to positively influence employee compliance. On the other hand, the combination of these measures limits the latitude of employees down to a level that triggers stress and strong negative emotions; hence leading towards reduced compliant behavior. Our framing provides increased compliant behavior and increased latitude.

Outlook

For the execution of this research, we plan to employ the factorial survey method. We do so for two main reasons: it reduces the experimental subject's desire to provide socially approved answers (i.e., social desirability bias), and it reduces his/her necessary effort. The former is achieved by asking subjects to judge based on the actions of actors within fictive scenarios, which bears little relation to the self and its social desirability (Chatterjee et al. 2015; Jarvenpaa and Staples 2001; Johnston et al. 2016; Siponen and Vance 2010; Vance et al. 2013, 2015; Willison et al. 2016). Explaining the latter requires further deliberations: The factorial survey is neither an experiment nor a traditional survey, yet it draws from both methods. From

traditional surveys, it draws the richness in detail and complexity, while orthogonality is drawn from experiments (Rossi and Nock 1982; Vance et al. 2015): Comparable to experiments, factorial surveys are constructed by designing certain dimensions (e.g., gender, empowerment, wrongdoing) of interest, which again consist of multiple levels, just like treatments within an experimental factor (Vance et al. 2015). The combination of one level of each dimension is called an object, which is operationalized in a (textual) vignette. The combination of all possible objects is referred to as vignette universe (Rossi and Nock 1982), with the objects being orthogonal with, correlations at, or close to, zero (Rossi and Nock 1982; Vance et al. 2015). This permits to draw random samples of one or more objects, for each experimental subject. Thus, each experimental subject needs to judge only one or few objects, but not all.

For the aforementioned reasons the factorial survey is sometimes also considered to be the gold standard to assess normative judgements on complex social phenomena (Seron et al. 2006; Vance et al. 2015). Based on this study's elaborations and results, it is feasible to employ this method and to pursue this endeavor in a full research paper, which is our intention.

References

Abdul Talib, Y. Y., and Dhillon, G. 2015. "Employee ISP Compliance Intentions: An Empirical Test of Empowerment," in *Proceedings of the Thirty Sixth International Conference of Information Systems*, Fort Worth, December, pp. 1–19.

Aguilar, L. A. 2015. "The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses," Public Statement, Public Statement, Washington D.C., USA: U.S. Securities and Exchange Commission, October, pp. 1–6. (https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html).

Ahearne, M., Mathieu, J., and Rapp, A. 2005. "To Empower or Not to Empower Your Sales Force? An Empirical Examination of the Influence of Leadership Empowerment Behavior on Customer Satisfaction and Performance.," *Journal of Applied Psychology* (90:5), pp. 945–955.

Balozian, P. Y. 2016. "The Downsides of Information Systems Security Policy Compliance Efforts: Toward a Theory of Unintended Reversed Security Action and Productivity (TURSAP).," Waco, Texas, USA: Baylor University. (https://baylor-ir.tdl.org/baylor-ir/handle/2104/9652/restricted-resource?bitstreamId=61767).

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change.," *Psychological Review* (84:2), pp. 191–215. (https://doi.org/http://dx.doi.org/10.1037/0033-295X.84.2.191).

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers & Security* (39:Part B), pp. 145–159.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *Management Information Systems Quarterly* (34:3), pp. 523–548.

Burg, D., and Waterfall, G. 2016. "Turnaround and Transformation in Cybersecurity: Key Fndings from The Global State of Information Security Survey 2016," Washington D.C., USA: PwC, pp. 1–32. (http://www.pwc.com/sg/en/publications/global-state-of-information-security-survey.html).

Chatterjee, S., Sarker, S., and Valacich, J. S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use," *Journal of Management Information Systems* (31:4), pp. 49–87.

Coleman, R. C. 2015. "2015 IC3 Annual Internet Crime Report," Annual Report, Annual Report, Washington D.C., USA: FBI Internet Crime Complaint Center, pp. 1–236. (https://www.ic3.gov/media/annualreports.aspx).

Conger, J. A., and Kanungo, R. N. 1988. "The Empowerment Process: Integrating Theory and Practice," *Academy of Management Review* (13:3), pp. 471–482.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285–318.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

Deci, E. L., and Ryan, R. M. 1985. *Intrinsic Motivation and Self-Determination in Human Behavior*, Rochester, New York: Plenum Press.

Deng, X., Joshi, K. D., and Galliers, R. D. 2016. "The Duality of Empowerment and Marginalization in Microtask Crowdsourcing: Giving Voice to The Less Powerful Through Value Sensitive Design," *Management Information Systems Quarterly* (40:2), pp. 279–302.

Garza, V., and Guo, X. 2015. "Securing BYOD: A Study of Framing and Neutralization Effects on Mobile Device Security Policy Compliance," in *Proceedings of the Thirty Sixth International Conference of Information Systems*, Fort Worth, December.

Györy, A. A. B., Cleven, A., Uebernickel, F., and Brenner, W. 2012. "Exploring the Shadows: It Governance Approaches to User-Driven Innovation," in *European Conference on Information Systems (ECIS) 2012*, Barcelona, Spain, June.

Harris, J., Ives, B., and Junglas, I. 2012. "IT Consumerization: When Gadgets Turn Into Enterprise IT Tools," *MISQ Executive* (11:3), pp. 99–112.

Harris, M. A., Patten, K., and Regan, E. 2013. "The Need for BYOD Mobile Device Security Awareness and Training," in *Proceedings of the Nineteenth Americas Conference on Information Systems*, Chicago, USA, August.

Jarvenpaa, S. L., and Staples, D. S. 2001. "Exploring Perceptions of Organizational Ownership of Information and Expertise," *Journal of Management Information Systems* (18:1), pp. 151–183.

Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research* (34:3), pp. 334–423.

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. 2016. "Dispositional and Situational Factors: Influences on Information Security Policy Violations," *European Journal of Information Systems* (25:3), pp. 231–251.

Junglas, I., Goel, L., Ives, B., and Harris, J. 2014. "Consumer IT at Work: Development and Test of an IT Empowerment Model," in *Proceedings of the Thirty Fifth International Conference on Information Systems*, Auckland, December, pp. 1–19.

Kirkman, B. L., and Rosen, B. 1999. "Beyond Self-Management: Antecedents and Consequences of Team Empowerment," *Academy of Management Journal* (42:1), pp. 58–74.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and H. Breitner, M. 2014. "Information Security Awareness and Behavior: A Theory-Based Literature Review," *Management Research Review* (37:12), pp. 1049–1092.

Lee, H., Jeon, S., and Zeelim-Hovav, A. 2016. "Impact of Psychological Empowerment, Position and Awareness of Audit on Information Security Policy Compliance Intention," in *PACIS*, Chiayi, Taiwan, July, p. 62.

Maruping, L. M., and Magni, M. 2012. "What's the Weather like? The Effect of Team Learning Climate, Empowerment Climate, and Gender on Individuals' Technology Exploration and Use," *Journal of Management Information Systems* (29:1), pp. 79–113.

Paternoster, R. 1987. "The Deterrent Effect of the Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues," *Justice Quarterly* (4:2), pp. 173–217.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law and Society Review* (30:3), pp. 549–584.

Ponemon, L. 2016. "2016 Cost of Data Breach Study: Global Analysis," Benchmark research, Benchmark research, Michigan, USA: Ponemon Institute LLC, June, pp. 1–31.

Potter, K., and Buchanan, S. 2016. "Coming to Terms With Business Unit IT to Prepare for Digital Business," Online: Gartner, Inc., April, pp. 1–6. (https://www.gartner.com/doc/3288932?refval=&pcp=mpe).

Pratt, T. C., and Cullen, F. T. 2005. "Assessing Macro-Level Predictors and Theories of Crime: A Meta-Analysis," *Crime and Justice*, pp. 373–450.

Putri, F. F., and Hovav, A. 2014. "Employees' Compliance with Byod Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory," in *European Conference on Information Systems (ECIS) 2014*, Tel Aviv, Israel, June.

Randolph, W. A. 1995. "Navigating the Journey to Empowerment," *Organizational Dynamics* (23:4), pp. 19–32.

Rossi, P. H., and Nock, S. L. 1982. *Measuring Social Judgments: The Factorial Survey Approach*, (1st ed.), California: SAGE Publications, Inc.

Seibert, S. E., Silver, S. R., and Randolph, W. A. 2004. "Taking Empowerment to the next Level: A Multiple-Level Model of Empowerment, Performance, and Satisfaction," *Academy of Management Journal* (47:3), pp. 332–349.

Seron, C., Pereira, J., and Kovath, J. 2006. "How Citizens Assess Just Punishment for Police Misconduct," *Criminology* (44:4), pp. 925–960.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *Management Information Systems Quarterly* (34:3), pp. 487–502.

Spreitzer, G. M. 1995. "Psychological Empowerment in the Workplace: Dimensions, Measurement, and Validation," *Academy of Management Journal* (38:5), pp. 1442–1465.

Thomas, K. W., and Velthouse, B. A. 1990. "Cognitive Elements of Empowerment: An 'interpretive' Model of Intrinsic Task Motivation," *Academy of Management Review* (15:4), pp. 666–681.

Thomson, G. 2012. "BYOD: Enabling the Chaos," *Network Security* (2012:2), pp. 5–8.

Tu, Z., and Yuan, Y. 2015. "Coping with BYOD Security Threat: From Management Perspective," in *Proceedings of the Twenty-First Americas Conference on Information Systems*, Puerto Rico, USA, August.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263–289.

Vance, A., Lowry, P. B., and Eggett, D. L. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *Management Information Systems Quarterly* (39:2), pp. 345–366.

Wallander, L. 2009. "25 Years of Factorial Surveys in Sociology: A Review," *Social Science Research* (38:3), pp. 505–520.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *Management Information Systems Quarterly* (37:1), pp. 1–20.

Willison, R., Warkentin, M., and Johnston, A. C. 2016. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives," *Information Systems Journal*.

Zhang, X., and Bartol, K. M. 2010. "Linking Empowering Leadership and Employee Creativity: The Influence of Psychological Empowerment, Intrinsic Motivation, and Creative Process Engagement," *Academy of Management Journal* (53:1), pp. 107–128.