FACTORS INFLUENCING FUTURE EMPLOYEES’ DECISION-MAKING TO PARTICIPATE IN A BYOD PROGRAM: DOES RISK MATTER?

Weeger, Andy, University of Applied Sciences Neu-Ulm, Neu-Ulm, Germany, andy.weger@hs-neu-ulm.de
Heiko, Gewald, University of Applied Sciences Neu-Ulm, Neu-Ulm, Germany, heiko.gewald@hs-neu-ulm.de

Abstract
As people use mobile devices (smartphones, tablets, etc.) more and more in daily life, their desire grows to use the same devices at work. In response to this demand, many firms are considering to offer BYOD programs allowing their employees to bring their own devices to work and use them for business purposes. This study analyses how employees’ perceive the benefits and risk associated with BYOD. Additionally, it is investigated whether innovativeness traits can serve as predictors of BYOD program participation. For this account, a theoretical model building on net valence approaches from decision making and perceived risk theory is proposed and tested. German students with relevant work experience and close to finishing their studies (i.e. future employees) were surveyed (n = 71).

The study demonstrates that benefits matter more than risks, at least for the suspected drivers of IT consumerization. The results show that the intention to enrol in a BYOD program is a function of perceived risk, perceived benefits and level of personal innovativeness. Among these factors, perceived benefit most strongly affects behavioural intention, whereas only safety risks proved to inhibit an individual’s intention to use privately-owned devices at work. Knowledge acquired from this study is particularly beneficial to IT executives to guide their decision to set up or adjust BYOD initiatives.

Keywords: IT consumerization, bring your own device (BYOD), perceived risk, generation me.

1 Introduction

Many people perceive that the devices, applications and services they use at home are easier to use than the information technology (IT) available at work (Harris and Junglas, 2011; Murdoch, Harris, and Dvore, 2010). Consequently, many of these employees want to use the same IT solutions in business and private contexts (BSI, 2013; Holtsnider and Jaffe, 2012), which lead to increasingly blurred boundaries between enterprise and private use of IT (BSI, 2013). As a result, firms find themselves overwhelmed by innovations aimed at the consumer sector spilling over into the corporate environment (Cummings, Massey, and Ramesh, 2009; Ingalsbe, Shoemaker, and Mead, 2011). This development is referred to as ‘consumerization of IT’. The topic “bring your own device” (BYOD) is closely related to IT consumerization (BSI, 2013). While IT consumerization refers to the dual use of all types of devices, applications and services (e.g. web-mail and cloud storage), BYOD focuses solely on hardware and refers to concepts where institutions allow or even encourage their employees to use their private devices for business purposes (BSI, 2013; Harris, Patten, and Regan, 2013). Since the advantages of mobile consumer technologies
such as intuitive user interfaces and appealing design—constantly change/increase employees' expectations towards IT in the firm, the relevance of BYOD increases (Weiß and Leimeister, 2012). In addition, using privately owned devices for business purpose provides employees with significant benefits like greater autonomy and better user experience (Harris and Junglas, 2011; Murdoch et al., 2010). As a consequence, the devices provided by the corporate IT department frequently do not meet employees' demand. Therefore, many employees use their own mobile devices to perform work related tasks even if the company does not encourages or permits to do so (Holtsnider and Jaffe, 2012).

In order to cope with this trend an increasing number of organizations officially established BYOD programs which enable their users to choose and use the devices that best meet their personal and business needs (Harris, 2012; Vogel, Kocoglu, and Berger, 2010). The primary motive for establishing BYOD programmes is usually to prevent the rise of shadow IT infrastructures (Györy, Cleven, Falk, and Brenner, 2012). Organizations additionally aim to establish safeguards for information security and manageability which are jeopardized by the business-use of privately owned devices (BSI, 2013; Györy et al., 2012). Usually, employees have to agree on a use-policy and the devices have to meet a set of specifications (Harris, Ives, and Junglas, 2013). Providing BYOD programs can therefore be seen as a strategy for mitigating risk in the organization.

BYOD is not per se beneficial for employees. Using privately owned devices for business purposes can, for example, threaten work-life balance and put the employee at risk of being responsible for corrupting the corporate network with malware etc. (Niehaves, Köffer, and Ortbach, 2012). The latter can result in consequences which are neither favourable for the organization, nor for the individual. However, implementing safeguards to prevent security breaches or unbalanced workload due to the dual use of private IT devices proves to be difficult (BSI, 2013). Therefore, offering a BYOD programs means that companies assign a high level of responsibility to their employees.

Prior research does not provide sufficient insight on employees’ sense of responsibility and on their risk awareness regarding BYOD. Addressing this gap, this study aims to investigate how risk perceptions and benefit expectations impact individuals’ intention to participate in a corporate BYOD program and, by implication, his or her intention to use private IT devices at work.

The paper is structured as follows. In the next section, we briefly discuss the background of this study encompassing IT consumerization, net-valence approaches in decision making and perceived risk theory. Based on these findings, the development of the research hypotheses is presented. Subsequently, we explicate the research design and data analysis end with a discussion of the results and implications.

2 Theoretical Background

BYOD is discussed as the unit of analysis of this study and related to the phenomenon of IT consumerization. Subsequently, we examine prior literature on theories aiming to explain decision-making mechanism at the individual level.

2.1 IT Consumerization and BYOD

IT consumerization is regarded as the consequence of a shift in the computerization process, which is triggered by employees who are pushing privately used IT solutions into the workplace (Baskerville, 2011; Weiß and Leimeister, 2012). Many scholars conceptualize IT consumerization as the dual use of consumer devices, applications and services for private and business purpose (Holtsnider and Jaffe, 2012; Ingalsbe et al., 2011). Niehaves et al. (2012) focus on ownership as the key-characteristic of IT consumerization. They define consumerization as a scenario at the intersection of private ownership and corporate deployment in which employees “invest own resources to buy, learn, and use consumer technology at their workplace” (p. 2). The question of 'ownership' is also the defining characteristic of BYOD. This concept refers to the paradigm where personally owned mobile devices are used for
business and private purposes. Although BYOD is a popular contemporary buzz acronym (Oliver, 2012) a commonly accepted definition has not yet emerged. The German Federal Office for Information Security defines BYOD as “strategies pursued by institutions to encourage their staff members to use their private devices for enterprise purposes or to even create financial incentives to do so” (BSI, 2013, p. 1). Consequently, BYOD can be classified as an organizational instantiation of IT consumerization, which is limited to the use of hardware devices.

Prior literature assumes that the perceived advantages of mobile consumer technologies encourage employees to use their privately owned mobile devices for business purposes (Holtsnider and Jaffe, 2012). It is expected that IT consumerization positively contributes to employee work performance by increasing satisfaction, flexibility and mobility (Niehaves, Köffer, and Ortbach, 2013). Notwithstanding, BOYD also involves risks like the obliteration of boundaries of professional and private life (Ingalsbe et al., 2011; Niehaves et al., 2012). Depending on the BYOD program’s financial model, participation could also impose financial risks on employees. Concepts like “choose your own device” (CYOD) enable the employee to select a device from a predefined shopping cart which is financed by the company (Lang, 2012); whereas “we sponsor your device” (WSYD) implies that the employee receives financial compensation for using a privately-owned device for business purposes (Vogel et al., 2010). In the latter case, employees participating in the BOYD program bear the financial risk of purchasing and maintaining the device for a period of time.

Organizational challenges of BYOD are intensively discussed in academia and practise (for a review see e.g. Niehaves et al., 2012). Research touching the perspective of employees is mostly limited to an enumeration of benefits and disadvantages, but does not examine if and how employees consider them when evaluating the use of private IT resources for business purpose. As discussed above, literature does assume that BYOD does involve benefits and risks for employees, but does not examine if these assumed advantages and disadvantages influence an individual’s intention to use private devices at work.

2.2 Net-Valence Models and Perceived Risk Theory

Social psychology provides net-valence models for investigating individual decision making. These models take individual benefit expectations and subjective cost perceptions into account. They assume that if benefits (positive valence) of a certain behaviour (e.g. using a service) do outweigh the costs (negative valence) an individual will tend to perform an action (Fishbein, 1967; Lewin, Dembo, Festinger, and Sears, 1944). Building on these theories, marketing research demonstrates that individuals accept expected negative utility (costs) in order to obtain expected positive utility (benefits) as long as the expected net utility is positive (see e.g. Peter and Tarpey Sr, 1975). Actions often produce consequences which cannot be quantitatively estimated. Following this argument, costs of a decision or behaviour have been primarily measured through risk perceptions (e.g. Campbell and Brown, 2005; Featherman and Fuller, 2003; Featherman and Pavlou, 2003; Liu, Yang, and Li, 2012). In contrast to approaches which evaluate risk from an objective manner, perceived risk conceptualizes negative utility from a subjective perspective. Perceived risk was introduced by Bauer (1967) in his perceived risk theory (PRT) which analyses the risk an individual associates with the consequences of a decision. The theory assumes that subjective risk perceptions directly impact an individual’s intention to perform a certain action (Cunningham, 1967). Perceived risk is defined as the subjective expectation of a possible loss (Stone and Gronhaug, 1993). PRT has been adopted in different disciplines to understand the effect of risk perceptions on consumers' behaviour (Bauer, 1967). Furthermore, perceived risk was found to be a significant determinant of an individual’s intention to use certain IT solutions (Featherman and Pavlou, 2003; Liu et al., 2012).

Usually, benefits are also evaluated from a subjective perspective and conceptualized as perceived benefit. Perceived benefits “include all benefits which the customer perceives as having been received” (Liljander and Strandvik, 1992, p. 15). In the context of IT, perceived benefit reflects the overall positive utility an individual expects when using a particular technology (Kim and Olfman,
Lee (2009) and Liu et al. (2012) demonstrated that perceived benefit also has a significant influence on behavioural intention.

3 Research Model

In the light of the afore-mentioned theoretical arguments, we propose a net-valence model for investigating an individual’s intention to participate in a corporate BYOD program.

Figure 1: Research Model

Prior research provides sufficient evidence that perceived benefit and perceived risk significantly determine an individual’s intention to adopt IT or technology-related services. Subsequently, the research model depicted in Figure 1 proposes that an individual's **behavioural intention** to participate in a corporate BYOD program is inhibited by his or her risk perceptions and positively impacted by the benefits he or she expects to receive. As this study puts a focus on individuals’ risk-perceptions, it includes the risk-facets proposed by perceived risk theory. In contrast to perceived benefits, perceived risk is therefore modelled as a formative second-order construct. The risk facets as proposed by PRT constitute the first-order variables of PRT. These risk facets and the other variables of the research model and their proposed causal relationships are discussed below.

Cunningham (1967) defines **perceived risk** as “the amount that would be lost (i.e. that which is at stake) if the consequences of an act were not favourable, and the individual's subjective feeling of certainty that the consequences will be unfavourable” (p. 85). Subsequently, we refer to perceived risk as to an individual's beliefs about the potential uncertain negative outcomes caused by participating in a corporate BYOD program.

Most scholars agree that the negative consequences of behaviour can be classified into different types of loss. Therefore, it is proposed that perceived risk is a kind of a multi-dimensional construct encompassing various dimensions (Featherman and Pavlou, 2003; Jacoby and Kaplan, 1972; Lee, 2009). Although these dimensions may vary according to the unit of analysis, each dimension can be viewed as perception of the probability of a future loss that, in turn, contributes to an individual's overall risk assessment (Sweeney, Soutar, and Johnson, 1999). Based on existing discussions about BYOD in academia and practice, we propose that perceived risk of BYOD includes financial, performance, psychosocial, security, privacy and safety risk facets (see e.g. Niehaves et al., 2012).

**Psychosocial risk** (PR-PS) encompasses psychological and social risk-facets (Cunningham, 1967). It accounts for the potential that an individual’s decision may produce negative effects on one’s peace of mind or self-perception (Mitchell, 1992) and that one’s social environment (e.g. friends, family, and
colleagues) will not value his or her decision (Featherman and Pavlou, 2003). Regarding BYOD, the company transfers the responsibility to select IT devices from the IT department to the employee. Hence, it is proposed that employees who perceive a high risk that their selection will negatively affect their self-perception or status are less comfortable selecting adequate devices, which in turn is a precondition for participating in a BYOD program. Transferring the technology decision to the employees also implies a shift of responsibility regarding the performance of the devices selected. In this regard, performance risk (RISK-PE) is “concerned with how well the product will perform relative to expectations” (Aldás-Manzano, Lassala-Navarré, Ruiz-Mafé, and Sanz-Blas, 2009, p. 56). Performance risk accounts for the potential that the device selected is not sufficient for its intended business purpose.

Participating in a BYOD program may also imply a financial risk (PR-FI). This is defined as “the potential monetary outlay associated with the initial purchase price as well as the subsequent maintenance cost” (Featherman and Pavlou, 2003, p. 1036). Financial risk is in particular relevant for BYOD programs based on the idea of “we sponsor your device”, where the employee is fully responsible that the financial compensation provided by the company is sufficient to ensure his or her working capacity during the given timeframe. The employee then bears the risk that actual costs for acquiring and more important maintaining the device may exceed the compensation.

Using an IT device for private and business purpose also entails the potential that personal information is disclosed to the employer without the employee's consent and knowledge (Miller, Voas, and Hurlburt, 2012). Capturing this issue, privacy risk (PR-PR) is defined as the “potential loss of control over personal information” (Featherman and Pavlou, 2003, p. 1036). Privacy risk does also capture the potential of losing private data due to a remote wipe of data performed by the employer in the case of device loss or user security compromise. As security breaches due to the use of private devices is a widespread threat (Niehaves et al., 2012), information security is one of the most important topics related to BYOD from the employer’s perspective. As a measure to safeguard security, BYOD programs usually encompass policies which delegate the responsibility for ensuring information security to the employer. Nonetheless, participating in a BYOD program increases the risk that the employee causes a security breach and that the employee harms the whole organization. In view of this arguments, security risk (PR-SE), defined as a potential loss due to fraud or a hacker compromising information security (Lee, 2009), is proposed to impact overall perceived risk.

Safety risk (PR-SA) accounts for effects which are incurring threats to an individual's health (Jacoby and Kaplan, 1972; Lu, Hsu, and Hsu, 2005). Prior consumerization research refers in particular to the potential to increase the stress level of employees (Niehaves et al., 2012). Being available outside working hours (e.g. due to using a smartphone for private and business purpose) may lead employees to abandon much of their off time to business, which in turn can lead to increased workload and stress. At worst, this has implications for the employee's health (e.g. burn out or other mental disorders).

Although the focus of this study lies on risk perception, perceived benefit has been included. Prior research conceptualized perceived benefit as the positive utility that an individual expects when adopting a particular IT and utilized perceived benefit as a direct determinant of IS adoption (Kim and Olfman, 2011). It was demonstrated that perceived benefit also positively impacts an individual's decision to adopt technology-related services (e.g. Lee, 2009; Liu et al., 2012). Furthermore, Porter and Donthu (2006) showed that users tend to overcome barriers if the benefits are substantive. Building upon these findings, we define perceived benefits as an individual's assessment of the benefits related to the usage of privately-owned devices at work. We propose that perceived benefit directly impacts his or her intention to participate in a corporate BYOD program.

Based on Rogers (1983) conceptualization of innovativeness, Agarwal and Prasad (1998) introduce personal innovativeness in the domain of IT (PIIT) as a construct characterizing adopters in the IT domain. They define personal innovativeness as the degree to which an individual is willing to adopt any new information technology. Personal innovativeness was found to impact an individual’s perceptions of a specific technology and his or her usage intention. Following these arguments, we
assume that people characterized by a high degree of personal innovativeness are more likely to use innovative IT devices for private and work-related activities and are therefore more likely to participate in a corporate BYOD program. Hence, we propose that personal innovativeness positively contributes to an individual’s behavioural intention.

4 Research Methodology

4.1 Instrument

To test the causal model, a questionnaire with a set of measurement items for each construct was developed. Measurement validity was safeguarded by adapting measurement items from prior research wherever possible. IS literature building on PRT provides a good repository of items which have been proved to deliver valid results (e.g. Aldás-Manzano et al., 2009; Featherman and Pavlou, 2003; Gewald and Dibbern, 2009). In order to relate the items to our unit of analysis, either the wording of the items was adapted or new items have been developed (in particular for privacy, security and safety risks). The items for measuring perceived innovativeness were adopted from Agarwal and Prasad (1998). Technically, perceived risk is measured as a second-order formative factor with first-order reflective constructs (the risk facets). For all other constructs reflective measurement modes have been applied. To test the validity of the measurement model, newly-developed and adapted items have been intensively tested within the research team and among students. All items have been measured on five-point Likert scales. Age, gender and course of studies have been included as control variables.

4.2 Data Collection and Sample

These days, IT consumerization is in particular evident in the lives of most young people (Carter, Thatcher, Applefield, and Mcalpine, 2011) who were born into the digital age where technology such as smartphones, web-services, and social media is ubiquitous (Prensky, 2001). Members of this generation are commonly referred to as ‘digital natives’ (Prensky, 2001) and they are frequently among the first to adopt new information technology. This is particularly obvious in educational settings, where their expectations on technology are shaped (Miller et al., 2012). Following this argument, students (i.e. future employees) can be seen as a driver of IT consumerization. Informal discussions with practitioners show that particularly young professionals demand using their own devices once they enter professional life. Understanding what drives young professionals’ decision to use privately-owned devices for private and work-related activities is of particular interest. Therefore, students in their last semesters have been selected as focus group for this study. To ensure a coherent set of responses and to limit the impact of external factors, undergraduate students of one German university with comparable and ‘technology-affine’ majors (information systems, industrial engineering, and business administration) have been chosen. All students already completed a mandatory practical semester (i.e. at least 6 months practical placement). Hence, they already acquired work-experience, which enables them to evaluate the benefits and risks of participating in a BYOD program.

Data was collected during a period of three weeks in April 2013 by distributing the standardized questionnaire using an online survey tool. To reduce the probability of nonresponse bias, the research team members regularly reminded their students to participate. In view of different ideas about BYOD among students, it was necessary to clarify the unit of analysis. Therefore, the type of BYOD program was outlined at the beginning of the questionnaire like this: Imagine your future employer permits you to use your private IT device(s) for work-related activities if you enrol in the BYOD program. Participating in this program means that you bear the costs for a/several mobile device(s) (e.g. a smartphone, notebook, tablet including necessary data plan) and that you agree to use the device(s) for work-related activities. For this purpose you will receive a financial compensation, which is fixed and accounts for a given time frame (e.g. $ 4,000 USD for 4 years). You are able to freely decide which devices you will use within this time frame. As your employer usually does not provide further devices, you are fully responsible for having sufficient IT equipment to get your job done.
Overall, 79 responses have been collected. These responses were reviewed and some initial quality measures have been applied. First, 8 responses with missing values have been excluded. Second, no significant differences between early and late respondents or outliers could have been found. This finding minimizes the chance of non-response bias. In total, 71 responses are retained for model evaluation. The sample consists of 27 male and 44 female students. The majority of students are between 22 and 25 years old (65%) and study information systems (71%).

4.3 Data Analysis

The model is tested using PLS\(^1\), a structural equation modelling method for complex predictive models and theory building (Barclay, Higgins, and Thompson, 1995; Lohmöller, 1989). Following previous literature (Chin, 2010; Gefen, Rigdon, and Straub, 2011; Hulland, 1999), PLS is a preferred analytical technique of this study for multiple reasons: PLS is in particular suitable for exploratory research, PLS does not require multivariate normality assumptions and it works well with small-to-medium sized samples (Gefen et al., 2011). A rule-of-thumb for PLS sample size is ten times the largest number of formative indicators used to measure one construct or ten times the structural equation (Barclay et al., 1995; Hair, Ringle, and Sarstedt, 2011). Perceived risk consists of six formative indicators, which is the largest number in this study. Hence, the sample exceeds the minimum suggested sample size of 60.

As perceived risk is modelled as a second-order formative factor with first-order reflective constructs, we followed the guidelines of Ciavolino and Nitti (2013) and applied the hybrid two-step approach. First, the measurement model of all constructs including the first-order variables of perceived risk are analysed using the repeated indicator approach. Second, testing the structural model, the factor scores of the first-order variables are applied as indicators for the second-order construct.

Before applying the hybrid two-step approach to evaluate the measurement and the structural model, we ran Harman’s single-factor test and conducted an exploratory factor analysis (Malhotra, Kim, and Patil, 2006; Podsakoff, MacKenzie, Lee, and Podsakoff, 2003). These analyses revealed the presence of multiple distinct factors with Eigenvalue greater than 1.0. This finding suggests that common method bias is not of great concern. Following prior literature, convergent validity of the measurement model was confirmed by meeting the following criteria (e.g. Gefen and Straub, 2005; Hulland, 1999): First, the loading of each item is significant and above the cut-off value of 0.60. Second, composite reliability (CR) of all constructs is above 0.70 and Cronbach’s alpha (CA) is above the cut-off value of 0.60 for exploratory measures. Finally, average variance extracted (AVE) of all constructs is above the threshold value of 0.50 (see Table 1).

<table>
<thead>
<tr>
<th>Construct</th>
<th>Mean</th>
<th>S.D.</th>
<th>AVE</th>
<th>CR</th>
<th>CA</th>
<th>Items</th>
<th>Loading t-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI</td>
<td>3.074</td>
<td>1.072</td>
<td>0.893</td>
<td>0.944</td>
<td>0.882</td>
<td>BI1 0.961*** 97.176</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BI2 0.929*** 28.730</td>
<td></td>
</tr>
<tr>
<td>PB</td>
<td>3.045</td>
<td>0.838</td>
<td>0.751</td>
<td>0.858</td>
<td>0.670</td>
<td>PB1 0.855*** 10.675</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PB3 0.878*** 10.445</td>
<td></td>
</tr>
<tr>
<td>PIIT</td>
<td>2.963</td>
<td>1.089</td>
<td>0.872</td>
<td>0.931</td>
<td>0.863</td>
<td>PIIT1 0.967*** 14.381</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PIIT2 0.899*** 9.950</td>
<td></td>
</tr>
<tr>
<td>PR-FI</td>
<td>2.905</td>
<td>0.766</td>
<td>0.733</td>
<td>0.846</td>
<td>0.636</td>
<td>RISK-PE1 0.922*** 35.572</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RISK-PE2 0.852*** 11.670</td>
<td></td>
</tr>
<tr>
<td>PR-PE</td>
<td>2.531</td>
<td>1.016</td>
<td>0.788</td>
<td>0.881</td>
<td>0.736</td>
<td>RISK-PE1 0.922*** 35.572</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) The software SmartPLS 2.0 (Ringle et al. 2005) was used to estimate the model and the bootstrap re-sampling method (71 cases; 5,000 samples; no sign changes) was used to determine the significance of the paths in the structural model.
Discriminant validity was also tested by ensuring that the correlations between constructs were below 0.85 (Brown, 2006) and that the square root of AVE for each construct exceeds the correlations between that construct and any other construct (Gefen and Straub, 2005). Thus, overall, our measures of the reflective constructs demonstrated good psychometric properties (see Table 2).

Finally, the following methods to safeguard the formative measurement model of perceived risk as second-order construct were applied. First, based on prior work on PRT it can be assumed that all relevant risk-facets have been considered. Second, content validity was established by discussing and sorting the measurement items among the research team. Third, significant path coefficients and variance inflation factors below 10 demonstrate a sufficient level of indicator validity (Chin, 1998). Fourth, the correlations between the formative and all the other constructs are less than 0.71, which indicates sufficient construct validity (MacKenzie, Podsakoff, and Jarvis, 2005). Last not least, construct reliability was tested using a two-construct model, that integrates an additional “phantom variable”, which represents the construct’s reflective operationalization (Diamantopoulos and Winklhofer, 2001). The test demonstrates a strong and significant relationship between the formative operationalization of perceived risk and the reflective phantom variable, which indicates sufficient construct reliability.

**Table 1:** Descriptive statistics, convergent validity, internal consistency and reliability

***Significant at the 1% level

<table>
<thead>
<tr>
<th>Construct</th>
<th>Mean</th>
<th>S.D.</th>
<th>AVE</th>
<th>CR</th>
<th>CA</th>
<th>Items</th>
<th>Loading</th>
<th>t-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISK-PE2</td>
<td>0.852***</td>
<td>11.670</td>
<td></td>
<td></td>
<td></td>
<td>RISK-PR1</td>
<td>0.897***</td>
<td>26.758</td>
</tr>
<tr>
<td>RISK-PR2</td>
<td>0.846***</td>
<td>13.749</td>
<td></td>
<td></td>
<td></td>
<td>RISK-PS1</td>
<td>0.907***</td>
<td>8.755</td>
</tr>
<tr>
<td>RISK-PS2</td>
<td>0.851***</td>
<td>5.090</td>
<td></td>
<td></td>
<td></td>
<td>RISK-PR1</td>
<td>0.897***</td>
<td>26.758</td>
</tr>
<tr>
<td>RISK-SA1</td>
<td>0.948***</td>
<td>57.924</td>
<td></td>
<td></td>
<td></td>
<td>RISK-PS1</td>
<td>0.907***</td>
<td>8.755</td>
</tr>
<tr>
<td>RISK-SA2</td>
<td>0.947***</td>
<td>51.853</td>
<td></td>
<td></td>
<td></td>
<td>RISK-PR1</td>
<td>0.897***</td>
<td>26.758</td>
</tr>
</tbody>
</table>

| Table 2: Inter-construct correlation matrix, square root of AVE shown in bold (diagonal)
Andy Weeger and Heiko Gewald / BYOD – Do Risk Perceptions Matter?

<table>
<thead>
<tr>
<th>Formative Items</th>
<th>Weight</th>
<th>t-score</th>
<th>VIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR-FI</td>
<td>0.108</td>
<td>0.467</td>
<td>1.099</td>
</tr>
<tr>
<td>PR-PE</td>
<td>0.419</td>
<td>1.551</td>
<td>1.166</td>
</tr>
<tr>
<td>PR-PR</td>
<td>0.390</td>
<td>1.503</td>
<td>1.391</td>
</tr>
<tr>
<td>PR-PS</td>
<td>-0.248</td>
<td>0.995</td>
<td>1.062</td>
</tr>
<tr>
<td>PR-SA</td>
<td>0.588*</td>
<td>2.311</td>
<td>1.205</td>
</tr>
<tr>
<td>PR-SE</td>
<td>-0.097</td>
<td>0.327</td>
<td>1.233</td>
</tr>
</tbody>
</table>

Table 3: Item weights, t-statistics and VIF per dimension of perceived risk

4.4 Results

The results of the structural model validation are presented in Figure 2. Significance level of the path coefficients is above 0.01 for all paths to behavioural intention. The independent variables account for about 31.8% of the variances in behavioural intention, which can be considered as moderate (Chin, 1998). Contrary to expectations, only safety risk significantly loads on perceived risk.

![Figure 2: PLS structural result (path coefficients are significant at the ** 1% level, * 5% level)](image)

Following the recommendation of (Chin, 1998), the blindfolding procedure with a common omission distance of 7 was carried out to calculate the Stone-Geisser Criterion ($Q^2$) for behavioural intention ($Q^2 = 0.228$). $Q^2$ exceeds the threshold value of 0.00 suggesting sufficient model validity.

<table>
<thead>
<tr>
<th>Path</th>
<th>Path-coefficient</th>
<th>t-score</th>
<th>Effect size ($f^2$)</th>
<th>Effect</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>PB -&gt; BI</td>
<td>0.308**</td>
<td>2,7934</td>
<td>0,123</td>
<td>Weak</td>
<td>Supportable</td>
</tr>
<tr>
<td>PIIT -&gt; BI</td>
<td>0.257**</td>
<td>2,7618</td>
<td>0,079</td>
<td>Weak</td>
<td>Supportable</td>
</tr>
<tr>
<td>PR -&gt; BI</td>
<td>-0.257*</td>
<td>2,4484</td>
<td>0,079</td>
<td>Weak</td>
<td>Supportable</td>
</tr>
</tbody>
</table>

Table 4: Results of PLS path analysis (significant at the ** 1% level, * 5% level)

Cohen’s $f^2$ (Cohen, 1988) for perceived benefits, perceived risk and personal innovativeness indicate rather weak effects on behavioural intention, whereas perceived benefits clearly reveals the strongest effect on intention. Table 4 depicts some quality measures of the structural model.
5 Discussion

Results indicate that the participating students consider both risks and benefits of taking part in a BYOD program. However, all independent variables have only weak effect on behavioural intention, whereby the effect of perceived risk ($f^2 = 0.079$) is significantly smaller than the effect of perceived benefits ($f^2 = 0.123$). These findings suggest that there are factors beyond perceived benefits, perceived risk, and personal innovativeness that are necessary to explain young professionals’ intention to participate in a BYOD program. Apart from the magnitude of effect, the direction of the influence of all dependent variables is as expected. Benefit expectations and innovativeness traits positively influence behavioural intention, whereby perceived risk inhibits the dual use of privately-owned devices. This finding supports the assumptions in prior literature that IT consumerization is mainly triggered by personal needs and benefit expectations (see e.g. Niehaves et al., 2012).

The formative conceptualization of perceived risk developed in this study allows us to evaluate the relative impact of each risk facet instead of treating risk as a black-box. This approach implies that – while the perceived risk is suggested to be multidimensional in nature – not all the dimensions are salient for shaping the intention of to-be employees to participate in BYOD programs. Considering the dimensions forming perceived risk, the majority of our findings are contradictory to our propositions. Only safety risk significantly contributes to the formation of perceived risk.

The controversial discussion in social psychology about the idea of a so called generation me could help explaining these results (for a recent discussion see e.g. Arnett, 2013). Generation me (also referred to as generation Y) comprises those born between the early 1980s and 2000 (Twenge, 2007) which largely reflects our sample. Twenge empirically shows that there is a rise of individualistic and narcissist traits within the generation me. Narcissism is, for instance, strongly linked to overconfidence and unrealistic risk taking (Foster, Shenesey, and Goff, 2009; Twenge and Campbell, 2008). Furthermore, narcissism is commonly related to benefits to the individual that are primarily affective and mostly short term orientated, whereas the cost of narcissism is usually borne by others (Campbell and Buffardi, 2008). This trait offers a possible explanation for the weak effect of perceived risk on behavioural intention. Furthermore, it explains comprehensibly why only safety risk contributes to the formation of perceived risk. If one assumes that the probability of negative financial effects when participating in a BYOD programme is minimal, only safety risk comprises potential negative outcomes which have to be borne immediately and solely by the risk-taker.

Implications for practise can be drawn from the results of this study. First, findings show that security risk does not significantly contribute to overall perceived risk, hence, has no significant effect on behavioural intention. This implies that security risks do not impact the decision making process to decide whether to enrol in a corporate BYOD program or not. Since young professional seem not to consider security risks, IT executives are well advised to take these risks seriously to implement sufficient measures to secure their network and data. For this purpose, IT executives need to set up adequate IT, security and training strategies to channel this trend. Managers may also develop new ways of managing corporate IT risks to address the missing security and privacy risk awareness. Second, this study suggests that benefit perceptions matter more than risk perceptions. This implies that if soon-to-be employees will perceive benefits from using their private-owned devices for work-related activities, they will most likely enrol in a BYOD program. Furthermore, descriptive analysis of the data reveals that our sample, on average, actually perceives benefits and tends to participate in

---

2 One could assume that if a device is broken and one is not able/willing to buy a new one, the company will step in order to ensure job performance. Therefore, an individual could assess the likelihood of negative financial effects as low. Furthermore, the amount given in the introduction of the questionnaire may play a part in contributing to the insignificant effect of the financial risk facet.
corporate BYOD programs. This finding may motivate IT executives to intensify their efforts in developing adequate BYOD strategies.

This study has certain limitations which need to be considered. First and foremost, the sample consists of students, not working professionals. Although the research objects have gained relevant work-experience and are expected to be drivers of IT consumerization once they enter into employment, they are not yet full-time employees. Furthermore, students with majors of affinity toward IT were selected. This is likely to result in a bias towards the demand of BYOD and therefore limit the generalizability of the results. Third, only a specific type of BYOD programs has been examined. Offering a compensation for using privately-owned devices at work may create some dynamics, which are different from other varieties of BYOD.

Building on the initial insights of this study, further research should focus on ‘real’ employees (i.e. young professionals - already working for at least a year) and different types of BYOD programs. Furthermore, alternative concepts and measurements of individual BYOD risk perception should be examined.

6 Conclusion

This paper provides new insights into individuals' risk and benefit perceptions as well as innovativeness traits as useful predictors of BYOD program participation. As such, this study sheds light on the drivers of IT consumerization. It empirically demonstrates that for the 'soon-to-be-employees' benefits matter more than risks as driver of IT consumerization. The results show that the intention to enrol in a BYOD program is a function of perceived risk, perceived benefits and personal innovativeness. Among these factors, perceived benefits most strongly affected behavioural intention, whereas only safety risks proved to inhibit an individual’s intention to use privately-owned devices at work. Knowledge acquired from this study is in particular beneficial to IT executives planning to set up or adjust their BYOD initiatives.

References


Harris, C. "Mobile Consumerization Trends & Perceptions - It Executive and Ceo Survey," Decisive Analytics, LLC.


Murdoch, R., Harris, J.G., and Dvore, G. "Can Enterprise It Survive the Meteor of Consumer Technology?," Accenture Institute for High Performance.


