ARE YOU READY TO LOSE CONTROL? A THEORY ON THE ROLE OF TRUST AND RISK PERCEPTION ON BRING-YOUR-OWN-DEVICE POLICY AND INFORMATION SYSTEM SERVICE QUALITY

Research in Progress

Ortbach, Kevin, University of Muenster, Muenster, kevin.ortbach@ercis.uni-muenster.de

Walter, Nicolai, University of Muenster, Muenster, nicolai.walter@ercis.uni-muenster.de

Öksüz, Ayten, University of Muenster, Muenster, ayten.oeksuez@ercis.uni-muenster.de

Abstract

IT consumerization or bring-your-own-device (BYOD) behavior, i.e., the use of private devices within organizational boundaries, is steadily increasing. Despite potential benefits, organizations are struggling to keep up with this development since a variety of risks, uncertainties, and potential costs are related to the use of private devices within the enterprise. Potential negative consequences are security breaches due to employees' lack of security measures or increasing coordination efforts for the IT department. While plenty of practitioner literature already exists, there is still a lack of scientific research. Especially theoretical foundations are lacking regarding organizations' decision processes underlying the implementation of BYOD policies, outcomes such as IS service quality, and the role of trust as an alternative to organizational and technical control mechanisms to minimize the risks associated with BYOD. Based on organizational trust literature, BYOD studies, and argumentations, we conclude a model of the influence of trust and risk perception on BYOD policies and outcomes. As a next step, we suggest a quantitative survey among Chief Information Officers (CIOs) to test the model. We conclude our study by outlining potential contributions to theory by integrating theories on organizational trust, IT risks, and IS service quality in the context of BYOD.

Keywords: Bring-your-own-device-behavior (BYOD), IT consumerization, Organizational Trust, Risks, BYOD Policy, IS Service Quality.

1 Introduction

IT consumerization or bring-your-own-device (BYOD) behavior, i.e., the use of private devices within the organizational boundary, is steadily increasing in organizations (Harris et al., 2012). Employees' expectations, e.g., with respect to performance, availability and ease-of-use of the services and technologies they use in the workplace, are influenced by their experiences in the private realm. With consumer-grade hardware and software getting more and more powerful, employees often use faster and more intuitive tools at home than at their workplace (Moschella et al., 2004). As a result, they are "increasingly abandoning enterprise IT (both hardware and software) in favor of consumer technologies that promise greater freedom and more fun" (Murdoch et al., 2010). Organizations are struggling to keep up with this development, resulting in dissatisfaction of employees (Harris et al., 2012) and the emergence of shadow IT (Behrens, 2009). They are forced to react to this trend by means of suitable policies that govern the use of privately-owned consumer IT in the enterprise.

While IS research has identified different strategies companies can pursue (Harris et al 2012), a theoretical perspective explaining BYOD policy choice is yet missing. In addition, IT consumerization has been found to be related to a variety of risks including security issues and loss of process control (Niehaves et al., 2012). BYOD has also been associated with an overload of the IT department and a related inability to provide support for the growing number of devices (e.g., Compuware 2011; Gens, Levitas, and Segal 2011). However, these relationships have not yet been analyzed empirically. While there are several practitioner-studies dealing with this topic, the majority is purely descriptive in nature and lacks a theoretical perspective. This lack of theory with respect to BYOD risks is surprising because a) BYOD has been seen as one of the most important IS trends (Gartner, 2013) and b) literature has already proposed mechanisms like mobile device management in order to deal with BYOD risks (Forrester, 2012). With respect to the latter aspect, most literature has focused on control mechanisms as reaction to the risks associated with IT consumerization and BYOD. However, research proposes trust to be another important factor dealing with risks in enterprises (Mayer et al., 1995). This perspective has been widely ignored with respect to BYOD so far in both research and practice.

Our research is focused on two major outcomes: 1) to provide a conceptualization of the relationship between trust and risk perception of CIOs, BYOD policy and internal outcomes in terms of information system service quality, and 2) to empirically examine these relationships using a survey among CIOs. The research question (RQ) for this study is:

> *RQ: What is the relationship between trust and risk perceptions of CIOs, their BYOD policy decisions and the information systems service quality within the company?*

In this paper, firstly, we present related work in the field. Secondly, discuss the development of a conceptual model that describes our emergent theory. Thirdly, we describe our proposed construct operationalization and measurement, and outline our methodology for empirically testing the model in upcoming research. Finally, we conclude with expected limitations and contributions.

2 IT Consumerization and BYOD

IT consumerization has been conceptualized as the adoption of consumer applications, tools and devices in organizations (Harris et al., 2012) and is commonly associated with a shift from the traditional top-down approach for IT provisioning to bottom-up IT innovation (Moore, 2011). In this context, Andriole (2012) speaks of a reverse technology-adoption life cycle. In literature, three distinct perspectives on the topic have been identified: 1) the employee perspective, which refers to an individual level view on private device and application usage in the work context, 2) the organizational perspective, which focuses on the growing number of non-approved and non-supported devices in the enterprise, and 3) the market perspective which sees IT consumerization to be related to all devices and applications in an enterprise that were initially developed for the consumer market (Harris et al., 2012). In this research we focus on the organizational perspective. Closely related to this perspective is the concept of BYOD, defined as a service offered by the organizational IT department that allows employees to bring privately owned devices to the workplace and to connect them to the corporate network in order to perform work tasks (Loose et al., 2013, p. 2).

Scientific literature on the emerging topics of IT consumerization and BYOD is scarce. Organizations are forced to establish suitable mechanisms and policies that govern the integration of consumer IT into the existing environment (D’Arcy, 2011; Moschella et al., 2004). However, to the best of our knowledge, no research exists on the decision process with respect to organizational BYOD strategies and the link between these strategies and potential outcomes. Most existing studies focus on the employee perspective on IT consumerization and develop models to explain the individual motivation behind using private IT at work. In addition, a plethora of practitioner reports has been published, primarily aimed towards pointing out potential benefits and threats (Niehaves et al., 2012). With respect to the latter, many studies have guided towards severe security and reliability risks associated with the growth of non-corporate IT (e.g. Harris, Ives, et al., 2011; Ingalsbe et al., 2011; Prete et al., 2011).

Regarding the former, increased employee satisfaction or cost reduction have been linked with the trend (Dell and Intel, 2011a, 2011b; Bradley et al., 2012; Avenade, 2012).

3 Trust and risk research in IS

The most common definition refers to trust as "the willingness of a party to be vulnerable [trustor; giving trust] to the actions of another party [trustee; receiving trust] based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al. ,1995, p. 712). Consequently, making oneself vulnerable involves taking a risk (Mayer et al., 1995). More precisely, risk is a requisite to trust (Deutsch, 1958) as the need for trust only arises in a risky situation (Mayer et al., 1995). In the field of economics there are two understandings of risks: 1) It can be a choice that entails a wide range of possible outcomes, or 2) a choice that contains a threat of negative outcomes only (March and Shapira, 1987). In the IS field, risk is usually understood with respect to the latter (e.g., Pavlou 2003). In this context, IT managers' risk perception may refer to the awareness of previous system violations (Straub and Welke, 1998). The process of taking an action in situations where perceived risks are present is called risk taking behavior (Mayer et al., 1995). The level of trust and perceived risk determines the degree of risk-taking in a relationship (Mayer et al., 1995). If the perceived risk is higher than the level of trust, individuals will look for alternatives to trusting, i.e., they will either try to not make themselves vulnerable or implement control mechanisms in order to reduce the perceived risk.

We assume that the trust perspective is particularly relevant in the context of BYOD due to two reasons: 1) BYOD strategy formation was found to be highly dependent on benefit and threat perceptions of the IT management (source forthcoming, anonymized for review version), suggesting that trust and risk are important factors, 2) BYOD is commonly associated with control mechanisms like mobile device management (Forrester, 2012). We believe that trust, as a natural counterpart to control, is worth to be investigated as an alternative mechanism to influence BYOD adoption behavior.

4 Model development

Our first approach at reaching an understanding of BYOD strategy formation and its impact on organizational outcomes is the development of a conceptual model structuring relevant factors and assisting the development of a novel substantial theory in this area. We take the established model of organizational trust by Mayer, Davis, and Schoorman (1995) as a basis for our theory framework. It suggests that an organizational *risk taking action* is influenced by *trust factors* and moderated by the *perceived risks* associated with the risk taking action. Establishing a BYOD policy can be regarded as risk taking action as an organization (as trustor) makes itself vulnerable to negative influences of BYOD such as security breaches (Harris et al., 2012). In turn, the risk taking action will yield organizational *outcomes*.

4.1 BYOD Trust Factors

In our model, we consider employees as trustees. Trust is a direct result of the assessment of trusting beliefs, i.e., the trustworthiness of another party. These trusting beliefs refer to ability, benevolence, and integrity (Mayer et al., 1995). First, ability refers to a "group of skills, competencies, and characteristics that enable a party to have influence within some specific domain" (Mayer et al. 1995, p. 717). Second, benevolence is considered as the degree to which a trustee acts in the trustor's interest aside from egoistic motives (Mayer et al., 1995). Finally, integrity describes the extent to which a trustor accepts the set of principles that guide a trustee (Mayer et al., 1995). Integrity usually refers to the extent a trustee is considered as truthful, honest, sincere and genuine (McKnight et al., 2002).

The assessment of employees' trustworthiness may take a leading role in the question of how to react to IT consumerization by means of a BYOD policy. In this context, competence or ability can be described as the extent to which employees are tech-savvy and have IT-skills to manage their devices.

Benevolence means that employees act in the interest of the company and do not intentionally harm the company. There is, for example, the risk that disgruntled employees exploit vulnerabilities associated with BYOD and do harm to the organization such as manipulation of certain transactions, data theft, or espionage (Straub and Welke, 1998). Integrity means that the employees share similar beliefs, the way of thinking of the IT department and other key decision makers with respect to BYOD and that they behave in a predictable manner. When the company believes that their employees bringing their devices are able to preserve the company from any harm, act benevolently by not intentionally doing harm to the company, than they will be perceive as trustworthy.

Proposition 1: The allowed level of BYOD in an organization depends on the IS management's trust in the employees.

4.2 Perceived BYOD Risk Factors

Risks can be defined as the "perceived severity of a threat" and the "perceived probability of the occurrence" of the threat (Herath and Rao 2009, p. 109). Most companies have their own information systems and, thus, are exposed to systems risks (Loch et al., 1992; Straub and Welke, 1998) defined as "the likelihood that an organization's information systems are insufficiently protected against certain kinds of damage or loss" (Straub and Welke 1998, p. 441). When companies allow their employees to use their private mobile devices for business operations or enable employees to access the companies' infrastructure via their private mobile devices, they have less control regarding the protection and security of the company's information system. This lack of control leads to higher perceived system risks. For example, the personal devices used by employees might be more vulnerable for system failures than the company's devices. The company is not able to control the stability of all devices used for business operations and thus hands over a lot of control to their employees and may trust them that they will not do any harm to the company, intentionally or unintentionally. Thus, it has to assess their employees' ability, benevolence, and integrity in order to decide whether to trust them or not.

In the model of organizational trust, perceived risks moderate the effect of trust on risk taking action (Mayer et al., 1995). If the level of trust is higher than the level of perceived risks, a risk taking action will result. If trust is not high enough a limited or no risk taking behavior will occur. Thus, the level of perceived risk as well as the level of trust determines the degree of risk a company is willing to take (Mayer et al., 1995). Thus, we propose:

Proposition 2: The influence of trust on the allowed level of BYOD is moderated by the IS management's perceived risks.

4.3 BYOD Policy (Risk Taking Action)

Literature suggests support for a relationship between the degree of BYOD and IS service quality: For instance, with respect to reliability, it has been found that consumer IT is often significantly less reliable than conventional IT equipment (Moschella et al., 2004), thus implying a negative effect. With respect to responsiveness, it can be expected that allowing BYOD will have a negative effect as well because BYOD has been associated with an increase in support complexity (Murdoch et al., 2010). For instance, it has been found that "more devices, times more apps, equals exponentially more complexity for IT to support and manage" (Gens et al., 2011, p. 4). Regarding assurance, implementing BYOD requires the IT department to have knowledge about all potential devices and applications that employees may bring to the company. Studies have shown that CIOs see this as almost impossible (Compuware, 2011), thus suggesting a negative effect of BYOD on assurance. With respect to empathy two effects are possible. On the one hand, BYOD is often associated with more individualization and needs fulfilment of the employees (Harris et al., 2012). On the other hand, employees usually expect the enterprise to provide suitable IT for work. However, in reference to consumer technologies, Harris et al. (2012) states that "the life cycle of these technologies is far shorter than what IT departments have grown accustomed to or can provide". Thus, BYOD may also have a negative impact on empathy. As for the last class of tangibles, consumer IT has been associated with more modern and appealing interfaces (Ortbach et al., 2013). Therefore, we propose:

Proposition 3: Outcomes in terms of service quality of the organizational IS depends on the level of allowed BYOD in the organization.

4.4 IS Service Quality (Outcome)

The implementation of BYOD is likely to have an effect on the overall quality of the IS service within a company. The most prominent concept to measure service quality is the SERVQUAL approach (Parasuraman et al., 1985) which has been adopted in the IS context to measure IS service quality (Jiang et al., 2002). It differentiates between five quality classes (Parasuraman et al., 1988, 1994): 1) reliability, which involves consistency of performance and dependability, 2) responsiveness, i.e., the ability to provide prompt service, 3) assurance, which is concerned with knowledge and courtesy of employees, 4) empathy, referring to individualized attention to customers, and 5) tangibles, being concerned with physical facilities and equipment. We will use these five classes as constructs for our dependent outcome factor.

Based on the stated literature and line of argumentation, we conclude the following model (Figure 1).

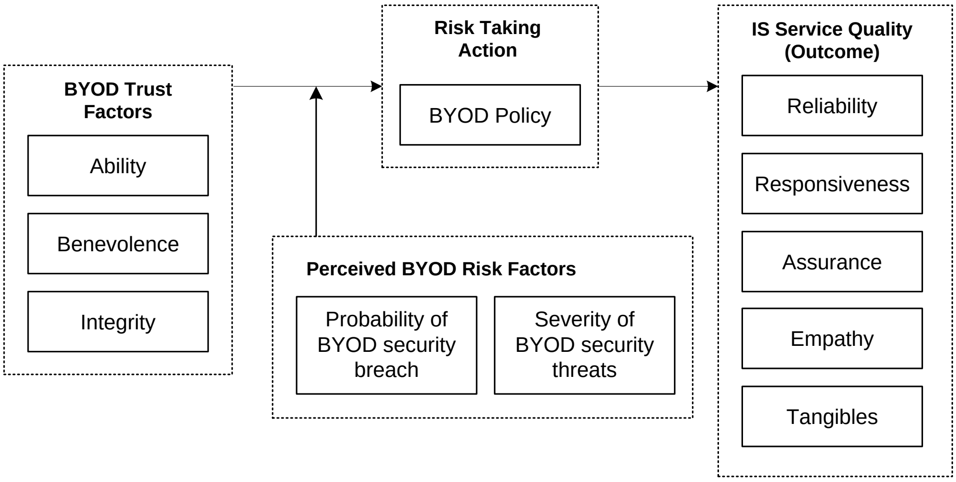

Figure 1. A Model of the Influence of Trust and Risk Perception on BYOD Policy and Outcomes

5 Research Design and Method

5.1 Study Design

To examine the research model, the survey has to be rolled out among IT decision makers. Thus, the sample should include IS executives from organizations that a) have a large share of employees who depend on technology use in their daily work, and b) operate in diverse markets and industries to allow for generalization of results. We have access to a mailing list of 600 CIOs, which meets these criteria. The list includes CIOs from small, medium, and large private organizations across all major industry sectors in Germany that have a high percentage of knowledge workers who heavily depend on IT usage in performing their work tasks.

In this context, we designed a mixed-method study combining several data collections (Tashakkori et al., 2012). First, we performed qualitative interviews with employees and IT managers in several companies as well as public sector organizations. Here, trust towards the employees as well as perceived risks with respect to security were identified as frequently mentioned factors influencing the BYOD decision among CIOs. In addition, increasing the satisfaction of the employees as well as the overall IS service quality was among the main goals. Second, based on these findings, we designed a quantitative survey which is presented in this paper. This quantitative research will be conducted in a two-step approach using a web based survey. First, we will perform a pre-test with a convenience sample of local CIOs that will not be included in the main study. The main data collection will then follow in two 'waves', each including half of the organizations on the mailing list. This will allow us to evaluate measurement instrument validity and reliability independently from the structural model and will also give us the opportunity to apply necessary changes to the propositions after the first data collection.

5.2 Operationalization of constructs

We operationalized our constructs by means of four different literature streams. First, we used organizational trust literature (Mayer et al., 1995) to define our three generic trust factors, i.e. ability, integrity, and benevolence of employees. Regarding the item measurement, we referred to the commonly used scale as developed by McKnight et al., (2002). Second, we used literature on IS security breaches (Herath and Rao, 2009) and adapted its constructs and items of probability and severity to the context of BYOD. Third, with respect to our risk taking behavior of implementing a BYOD policy, we draw on BYOD literature as the concept has recently been introduced and operationalized (Ortbach et al., 2014). Fourth, we use the five SERVQUAL dimensions of reliability, responsiveness, assurance, empathy and tangibles (Parasuraman et al., 1994) and adapt their items to match the BYOD context of our study.

Table 1 provides an overview of the factors and constructs of our research model and their definitions based on the literature.

Factor	Construct	Definition
Trust *(Mayer et al., 1995)*	Ability	The degree to which employees have skills and competencies to manage their personal devices.
	Benevolence	The degree to which employees act in the interest of the organization and not just their own.
	Integrity	The degree to which employees adhere the principles of their organization.
Perceived Risk (Herath and Rao, 2009; Milne et al., 2000)	Probability of BYOD security breaches	The degree of how personally susceptible an organization feels to security threats caused by BYOD.
	Severity of BYOD security breaches	The degree of harm associated with the threats caused by BYOD.
Risk taking behavior (Ortbach et al., 2014)	BYOD Policy	The degree to which an organization allows the use of private devices for work tasks.
IS Service Quality (Outcomes) (Jiang et al., 2002; Parasuraman et al., 1985)	Reliability	The ability of an organization to perform the promised IS services dependably and accurately.
	Responsiveness	The willingness and ability of an organization to help employees with IS related issues and provide prompt IS service.
	Assurance	The knowledge and courtesy of an organization with respect to the IS service provision.
	Empathy	The degree of attention within an organization towards the employees' needs with respect to IS services.
	Tangibles	The level of modernity and pleasurable appearance of the provided IS equipment and services.

Table 1. Construct Operationalization.

Based on these concepts, we developed a measurement instrument for use within our study. Table 2 provides an overview of this instrument and the related item sources.

Construct	Item Definition
Ability *(McKnight et al., 2002)*	TBA1: Our employees are competent and effective in managing their personal devices. TBA2: Our employees perform their role in managing their personal devices very well. TBA3: Overall, our employees are capable and proficient managers of their personal devices. TBA4: In general, our employees are very knowledgeable about their personal devices.
Benevolence *(McKnight et al., 2002)*	TBB1: I believe that our employees act in the best interest of our organization. TBB2: If our organization required help, our employees would do their best to help. TBB3: Our employees are interested in the well-being of our organization, not just their own.
Integrity *(McKnight et al., 2002)*	TBI1: Our employees are truthful in their dealings with our organization. TBI2: I would characterize our employees as honest. TBI3: Our employees would keep their commitments. TBI4: Our employees are sincere and genuine.
Probability of BYOD security breach (Herath and Rao, 2009)	STP1: How likely is it that BYOD will cause a significant outage that will result in loss of productivity? STP2: How likely is it that BYOD will cause a significant outage that results in financial losses to the organization? STP3: How likely is it that the organization will lose sensitive data due to BYOD?
Severity of BYOD security threats (Herath and Rao, 2009)	STS1: I believe that information stored on organizational computers is vulnerable to security incidents caused by BYOD. STS2: I believe the productivity of the organization and its employees is threatened by security incidents caused by BYOD. STS3: I believe the profitability of the organization is threatened by security incidents caused by BYOD.
BYOD Policy (Ortbach et al., 2014)	BDC1: Our organization allows employees to use their private devices for business operations. BDC2: Our organization enables employees to access the enterprise infrastructure via their private devices. BDC3: Our organization promotes the use of private devices within the business context.
Reliability (Parasuraman et al., 1994)	REL1: Our organization provides IS services as promised. REL2: Our organization is dependable in handling employees' IS problems. REL3: Our organization provides IS services right the first time. REL4: Our organization is able to provide IS services at the promised time. REL5: Our organization maintains error-free records with respect to its IS services
Responsiveness (Parasuraman et al., 1994)	RES1: Our organization keeps the employees informed about the IS services. RES2: Our organization gives prompt IS services to its employees. RES3: Our organization is willing to help employees with IS problems. RES4: Our organization is ready to respond to employees' IS requests.
Assurance (Parasuraman et al., 1994)	ASS1: Our organization can instill confidence with respect to IS services in employees. ASS2: Our organization makes employees feel safe with respect to their IS. ASS3: Our organization is consistently courteous when it comes to providing IS services. ASS4: Our organization has the knowledge to answer employees' questions with respect to the IS services.

Empathy (Parasuraman et al., 1994)	EMP1: Our organization gives its employees individualized IS services. EMP2: Our organization deals with the employees in a caring fashion when it comes to providing them with IS services. EMP3: Our organization has the best interest of the employees at heart when providing them with IS services. EMP4: Our organization understands the needs of the employees with respect to IS services. EMP5: Our organization IS services can be accessed conveniently.
Tangibles (Parasuraman et al., 1994)	TAN1: The employees of our organization work with modern IS equipment. TAN2: The employees of our organization work with visually appealing IS. TAN3: The employees of our organization work with IS that have a neat and professional appearance. TAN4: Our organization provides visually appealing materials associated with the IS service.

Table 2. Suggested Measurement Instrument

6 Expected Contributions

We expect our research to make significant contributions to theory by integrating theories on organizational trust, IT risks, and organizational IS service quality in the context of BYOD and IT consumerization. First, our research conceptualizes trust and risk factors in the context of BYOD and their relationship with the BYOD policy. This is expected to contribute to the ongoing discussion on IT consumerization strategies (Harris et al. 2012) by investigating the reasons behind managerial decisions with respect to BYOD from the perspective of trust and risk theory. In particular, we expect our study to provide meaningful insights into which factors are most influential on the BYOD decision of CIOs. Second, trust is evaluated as an alternative to control mechanisms. While control mechanisms like mobile device management were shown to be affected by perceived risks with respect to BYOD (Ortbach et al., 2014), it will be interesting to see whether or not trust factors may be used to explain BYOD policy decisions. Moreover, it can be analyze which of these factors have the highest impact. Determining trust factors influencing the decision of CIOs will be the first step towards developing measures to build a company culture that accepts and supports employee autonomy with respect to IT. Finally, our research contributes to theory in linking the concept of BYOD policy with particular outcomes in terms of IS service quality. While several of these relationships have been proposed by practitioner literature on IT consumerization (e.g., Gens et al. 2011; Moschella et al. 2004), our study is first to investigate their impact in detail by means of a quantitative study. From a managerial perspective, an analysis with respect to this impact of BYOD on the internal IT service quality and its subareas is very useful as it allows for determination of positive and negative effects regarding different quality dimensions. Furthermore, it allows for an estimation of the organizational impact and value of BYOD which may assist in developing suitable governance mechanisms in organizations.

References

Andriole, S.J. (2012), “Managing Technology in a 2.0 World”, *IT Pro*, No. January / February, pp. 50–57.

Avenade. (2012), *Global Survey: Dispelling Six Myths of Consumerization of IT.*

Behrens, S. (2009), “Shadow Systems: The Good, The Bad and the Ugly”, *Communications of the ACM*, Vol. 52 No. 2, pp. 124–129.

Bradley, J., Loucks, J., Macauley, J., Medcalf, R. and Buckalew, L. (2012), *BYOD: A Global Perspective. Harnessing Employee-Led Innovation*, San José, CA, USA.

Compuware. (2011), *Can IT win the race against change?*, Detroit, Michigan, USA.

D’Arcy, P. (2011), *CIO Strategies for Consumerization: The Future of Enterprise Mobile Computing*, Dell CIO Insight Series.

Dell and Intel. (2011a), *The Evolving Workforce: Expert Insights*, Round Rock, Texas, USA.

Dell and Intel. (2011b), *The Evolving Workforce: The Workforce Perspective*, Round Rock, Texas, USA.

Deutsch, M. (1958), "Trust and Suspicion", *The Journal of Conflict Resolution*, Sage Publications, Inc., Vol. 2 No. 4, pp. 265–279.

Forrester. (2012), *Mobile Device Management Underpins A Bring-Your-Own- Device (BYOD) Strategy*, Cambridge, MA, USA: A Custom Technology Adoption Profile Commissioned By Sybase/SAP.

Gartner. (2013), "Gartner Identifies the Top 10 Strategic Technology Trends for 2014", *Press release*, available at: http://www.gartner.com/newsroom/id/2603623 (accessed 23 November 2014).

Gens, F., Levitas, D. and Segal, R. (2011), *2011 Consumerization of IT Study: Closing the Consumerization Gap*, Framingham, Massachusetts, USA: IDC.

Harris, J.G., Ives, B. and Junglas, I. (2011), *The Genie Is Out of the Bottle: Managing the Infiltration of Consumer IT Into the Workforce*, Accenture Institute for High Performance.

Harris, J.G., Ives, B. and Junglas, I. (2012), "IT Consumerization: When Gadgets Turn Into Enterprise IT Tools", *MIS Quarterly Executive*, Vol. 11 No. 3, pp. 99–112.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106–125.

Ingalsbe, J.A., Shoemaker, D. and Mead, N.R. (2011), "Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise–an overview of considerations", *AMCIS 2011 Proceedings*, available at: http://aisel.aisnet.org/amcis2011_submissions/359/ (accessed 1 February 2012).

Jiang, J., Klein, G. and Carr, C. (2002), "Measuring information system service quality: SERVQUAL from the other side", *MIS Quarterly*.

Loch, K.D., Carr, H.H. and Warkentin, M.E. (1992), "Threats to information systems: today's reality, yesterday's understanding", *MIS Quarterly*, pp. 173–186.

Loose, M., Weeger, A. and Gewald, H. (2013), "BYOD–The Next Big Thing in Recruiting? Examining the Determinants of BYOD Service Adoption Behavior from the Perspective of Future Employees", *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Chicago, IL, USA, pp. 1–12.

March, J.G. and Shapira, Z. (1987), "MANAGERIAL PERSPECTIVES ON RISK AND RISK TAKING", *Management Science*, INFORMS: Institute for Operations Research, Vol. 33 No. 11, pp. 1404–1418.

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995), "An Integrated Model of Organizational Trust", *Academy of Management Review*, Vol. 20 No. 3, pp. 709–734.

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002), "Developing and validating trust measures for e-commerce: An integrative typology", *Information Systems Research*, Vol. 13 No. 3, pp. 334–359.

Milne, S., Sheeran, P. and Orbell, S. (2000), "Prediction and Intervention in Health Related Behavior: A Meta analytic Review of Protection Motivation Theory", *Journal of Applied Social Psychology*, Vol. 30 No. 1, pp. 106–143.

Moore, G. (2011), *Systems of Engagement and The Future of Enterprise IT - A Sea Change in Enterprise IT*, Silver Spring, Maryland, USA: AIIM.

Moschella, D., Neal, D., Opperman, P. and Taylor, J. (2004), *The "Consumerization" of Information Technology*, El Segundo: CSC Research White Paper.

Murdoch, R., Harris, J.G. and Devore, G. (2010), *Can Enterprise IT Survive the Meteor of Consumer Technology?*, Accenture Institute for High Performance.

Niehaves, B., Köffer, S. and Ortbach, K. (2012), "IT Consumerization – A Theory and Practice Review", *Proceedings of the Americas Conference on Information Systems*, Seattle, Washington, USA.

Ortbach, K., Brockmann, T. and Stieglitz, S. (2014), “Drivers for the Adoption of Mobile Device Management in Organizations”, *Proceedings of the 22nd European Conference on Information Systems*, pp. 1–18.

Ortbach, K., Köffer, S., Bode, M. and Niehaves, B. (2013), “Individualization of Information Systems - Analyzing Antecedents of IT Consumerization Behavior”, *Proceedings of the International Conference on Information Systems (ICIS)*, Milano, ITA.

Parasuraman, A., Zeithaml, V. and Berry, L. (1994), “Alternative scales for measuring service quality: a comparative assessment based on psychometric and diagnostic criteria”, *Journal of retailing*, Vol. 70 No. 3, pp. 201–230.

Parasuraman, A., Zeithaml, V.A. and Berry, L.L. (1985), “Model Service Its Quality and Implications for Future”, *Journal of Marketing*, Vol. 49 No. 4, pp. 41–50.

Parasuraman, A., Zeithaml, V.A. and Berry, L.L. (1988), “SERVQUAL: A Multiple-Item Scale for Measuring Consumer Perceptions of Service Quality”, *Journal of Retailing*, Vol. 64 No. Spring, pp. 12–40.

Pavlou, P.A. (2003), “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model”, *International Journal of Electronic Commerce*, Vol. 7 No. 3, pp. 101–134.

Prete, C. Del, Levitas, D., Grieser, T., Turner, M.J., Pucciarelli, J. and Hudson, S. (2011), *IT Consumers Transform the Enterprise: Are You Ready?*, Framingham, Massachusetts, USA: IDC.

Straub, D.W. and Welke, R.J. (1998), “Coping With Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly*, Vol. 22 No. 4, pp. 441–469.

Tashakkori, A., Teddlie, C. and Sines, M. (2012), “Utilizing mixed methods in psychological research”, *Research Methods in Psychology*, Wiley, New York, pp. 428–450.