BYOD-enabled workarounds: a process perspective

Emergent Research Forum Paper

Alina Dulipovici
HEC Montréal
alina.dulipovici@uqtr.ca

Dragos Vieru
Université du Québec
dragos.vieru@teluq.ca

Abstract

Bring Your Own Device (BYOD) is a very popular trend in the corporate world despite some paradoxical characteristics and scarce research on this topic. Drawing on the theoretical lens of workarounds, this paper proposes a dynamic explanation of BYOD-enabled workarounds. Specifically, we develop a conceptual model representing the multi-level process model that occurs when an IS-enabled practice enacted with an organizational device is replaced by a BYOD-enabled workaround. We claim that three outcomes are then possible: status quo, reverting to the organizational practice, or legitimizing the BYOD-enabled workaround as the new organizational practice. Moreover, we explain the conditions that regulate the proposed model.

In addition to addressing an important research gap, this study clarifies how and why several employers feel that they cannot prevent employees from using a BYOD approach. If a mix of conditions is already in place, there isn't indeed much to do, but to embrace the reality.

Keywords*:* BYOD, Workaround, Process Model, Conceptual Model, Shadow IT.

Acknowledgements

The authors would like to gratefully acknowledge the SSHRC funding received for this project.

Introduction

Since 2009 a new trend has gained popularity in the corporate world: 'bring your own device' or BYOD (Maddox, 2015). It is an alternative work strategy where employees bring their own computing devices such as laptops, smartphones, and/or tablets into the organization network in order to execute enterprise applications and to access organisational data rather than using company-owned devices (French et al., 2014; Ogie, 2016). The phenomenon responds to new work strategies (mobility, telecommuting, etc.) and to new ways of using information technology (IT), especially by the Millennials who have started to enter the labor market (Weeger et al., 2015). Organizations are willing to embark into this technological shift hoping it would bring economies of scale and scope as well as a positive image in the eyes of its employees by portraying an innovation-fostering organization with openness to technological advancement (Cook et al., 2013; Weeger et al., 2015).

Allowing BYOD initiatives comes with several potential threats for the organization: information system (IS) security, confidentiality of corporate information, employees' privacy, compliance, control, etc.

(Maddox, 2015). Nevertheless, many employers cannot really prevent employees from using their personal devices for business purposes; in this context, embracing this reality becomes the best option (Cidon, 2015). 74% of organizations of all sizes (compared to 62% in 2013) either already allow or plan to allow employees to bring their own devices to work (Maddox, 2015).

Despite its growing popularity, BYOD remains a paradoxical concept (Mokosch et al., 2015): employees have greater freedom, but also greater responsibility; the IT department delegates to a certain extent management responsibility to IT users within the organization, but it also has extra workload to protect its IT environment. According to Li et al. (2005) this kind of delegation significantly enhances flexibility and scalability, but reduces an organization's power and control. Employees using BYOD approaches can now work everywhere, any time, and not necessarily following organizational norms and constraints. According to prior research (Orlikowski, 1996; Pavlou and El Sawy, 2010), such a work environment is conducive to the emergence of unplanned processes (improvisation or workarounds) in order to fulfill daily tasks.

To our best knowledge, research on the relationship between utilization of BYOD, as a means to create a workaround, is rather scarce and has focused primarily on identifying BYOD-related factors that may lead to the enactment of a workaround or that my predict the intention to enact a workaround (Chua et al., 2014; Walters, 2013; Johnson, 2013). In the organizational context, a *workaround* represents a goal-driven change to an existing work system in order to overcome a technical or an organizational constraint (Alter, 2014). Our study conjectures about both effective and ineffective BYOD-based workaround practices. It seeks to provide "an explanation of how, why, and when things happened, relying on varying views of causality and methods for argumentation" (Gregor, 2006, p. 619). To do so we engage in theory development and propose a multi-level process-based conceptual model to answer the following question: *How key organizational and individual conditions affect the relationship between BYOD-enabled workaround practices and their related organizational practices?*

Theoretical Foundation

Representing a theory-building effort, we concentrate less on a complete review of the extant literature and put more emphasis on theoretical development (Rivard, 2014). One of our key building blocks is Alter's (2014) theory of workarounds that presents different perspectives on situations in which actors will either enable or intentionally perform actions going against one or more routines, instructions, expectations, prerequisites, specifications or organizational regulations. Organizations will generally perceive workarounds as unwanted processes (Azad and King, 2012), but they could also be a source of innovation and lead to a desirable outcome (Alter, 2014). The persistence of workarounds in a work environment is explained by the need for balance between bottom-up constraints (operationalization of the daily tasks) and top-down pressures (regulatory entities, physical constraints) (Azad and King, 2012). Organizational challenges linked to workarounds are due to a combination of different perspectives on workarounds. These perspectives are comprised of the ability to operate despite the obstacles, adopt an interpretative flexibility, balance between personal, group, organizational and authorized interests and learning emerging changes (Alter, 2014). In this context, we conjecture that, due to the perceived empowerment over the means to accomplish their work, employees using BYOD may attempt to achieve daily tasks through the establishment of workarounds. Next, we describe the conceptual model proposed.

Conceptual Model

Drawing on the theoretical lens of workarounds (e.g., Alter, 2014; Röder et al., 2014a), we develop a conceptual model (see figure 1) representing the multi-level process model that occurs when an when a practice enabled by an organizational-owned device is replaced by a BYOD-enabled workaround. We claim that three outcomes are then possible:

- The employee enacts and re-enacts the BYOD-enabled workaround without ever being detected by the organization;
- The employee is reprimanded for his workaround and he returns to the initial practice; or
- The workaround has a positive effect leading to some form of improvement of the business process, first, at the individual level, and then at the organizational level.

Several conditions (marked A, B, and C in figure 1) regulate the proposed process.

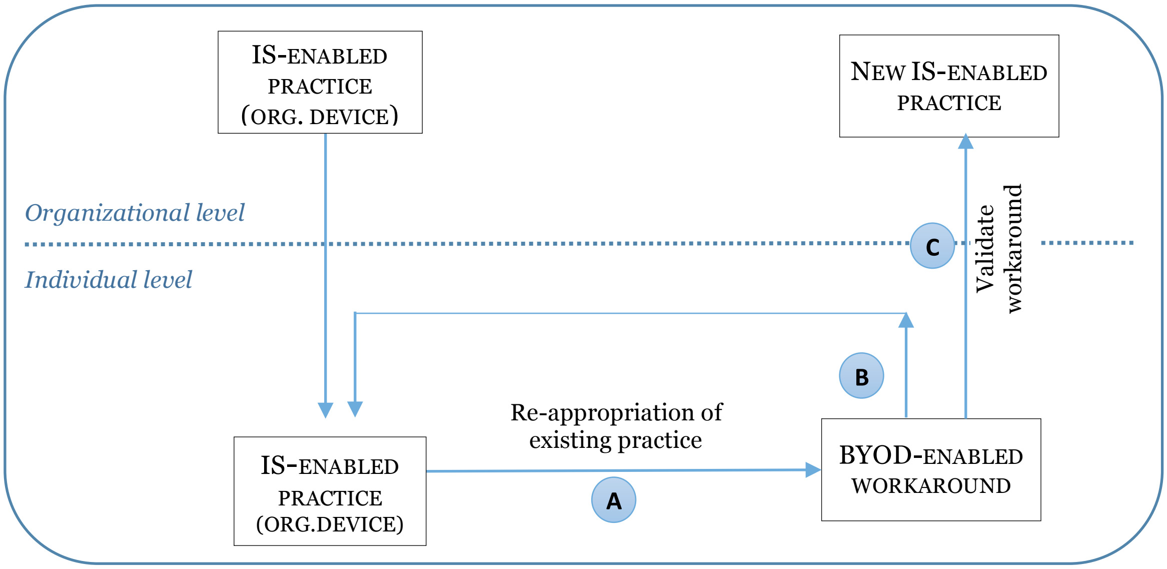

Figure 1: Conceptual model for BYOD-enabled workarounds

For symmetry and completeness, the model starts at the organizational level, when an organization implements a certain practice requiring the use of a technological device provided by the organization. In line with Röder et al. (2014a), we focus on work practices as process-instance-level routines (i.e. compared to a process-level routine, which is enacted only once). Process-instance-level routines are enacted by the situational factors and, given their repeatable nature, engagement with these practices affects the employee's willingness to enact a workaround (Röder et al., 2014a). For instance, following the implementation of a Microsoft SharePoint-based portal, employees are required to use their PCs to connect to the portal, and to access and store a variety of organizational documents (example, organizational memos and documents, reports and analyses, client lists, or the employees' directory). In order to prepare a report for a board meeting, managers could access reports stored on the portal and then synthesize or aggregate the data from these reports. Thus, employees use organizational resources (including the technological devices provided by the organization) to perform their regular tasks in process-instance-level routines.

Conditions A: When an employee re-appropriates an existing practice to enact a BYOD-enabled workaround

At the individual level, employees enact organizational-level practices. However, given the ubiquity of IT and the recent development of mobile computing with personal devices such as tablets and smartphones, many employees choose to perform office work with non-standard applications (Walters, 2013). As such, these employees adapt or re-appropriate an existing practice in new ways, by changing the device normally used to perform the existing practice. A manager from our previous example would like to access and prepare his report for a board meeting using an iPad or an iPhone. Our model focuses on the device, but Chua et al. (2014) found evidence of users who changed both the device and the application used.

According to prior research, re-appropriation of an existing IS-enabled practice occurs when employees have certain demands that the organization (for instance, the IT department) cannot fulfill because of budgetary or technical constraints (Chua et al., 2014). Hence, the existence of a specific *need* combined with the *inability of the organization to address that need* by replacing the device initially required with a different device become the first conditions triggering the re-appropriation of an existing practice. Other conditions facilitating the enactment of a BYOD-enabled workaround should also exist. Chua et al. (2014) talk about opportunity or the presence of a *conducive organizational environment,* such as an environment where policies do not exist or are not necessarily reinforced (Anonymous, 2013), where a security culture is weak or does not exist (Ruighaver et al., 2007), or where a strong culture of innovativeness with respect to technology exists (Koeffer et al., 2015). The presence of one or more of these conditions facilitate the enactment of a BYOD-enabled workaround practice in the shadow of the official practices and, more importantly, without consulting the IT department and without considering the integration with existing systems, the privacy and the security implications, as well as legal implications (Johnson, 2013).

With regard to the particular profile of the employee who enacts a BYOD-enabled workaround practice, *personal innovativeness* appears to be an important driver for this behavior (Ortbach, 2015; Röder et al., 2014a). "BYOD is driven by innovative employees that are technological early adopters in their private life and know about the features of their private IT and how it may be utilized for work purposes" (Ortbach, 2015, p. 1). Such *knowledge about the device* is clearly a necessary condition, but we claim that it is not sufficient. The employee needs to feel *a certain level of satisfaction* by using the personal device in his private life and he needs to *expect a benefit* from using his device for work. Röder et al. (2014a) found evidence that, before enacting a workaround, employees conduct a risk-benefit analysis in terms of expected efficiency gains and in terms of risks of process violations. Only if benefits outweigh risks, employees will act on their intention to create a workaround. Finally, the employee tends to self-legitimize his intention to enact a workaround in the shadow, if he *believes that the workaround amends a weakness* within the underlying business process (Röder et al., 2014b).

Conditions B: When an employee returns to the original practice

The return loop can be triggered by the organization (or the IT department in particular) or by the employee himself. In the first case, workarounds in the shadow are detected (especially if more than one employee enact the workaround) and the organization has to take appropriate action to punish the violation and to replace the workaround with the original practice because the *organization cannot allow* the workaround, for example, for security reasons, or *does not recognize the need for a different device* (Chua et al., 2014). It may be possible for the BYOD-enabled workaround *to be tolerated for a while by management* before appropriate action is taken. In that case, management perceives an efficiency gain and is willing to tolerate the BYOD-enabled workaround as long as this efficiency gain is plausible and security compliance is not at stake (Chua et al., 2014; Röder et al., 2014a).

In the second case, given some new information (for example, a better understanding of how the personal device is used for work purposes: our manager may be happy to write his report on his iPad, but realizes that his children also use the same iPad at home and may inadvertently access and disclose confidential information on social media), the employee may reassess his risk-benefit analysis and concedes that he *misjudged the benefits or the risks* in his initial risk-benefit analysis (Röder et al., 2014a). Thus, the risks of the violation being detected outweigh the benefits now and the employee decides to revert to the regular practice, before the BYOD-enabled workaround becomes a control failure and management has to take appropriate action to punish the violation.

Finally, it is also possible for an employee to enact a BYOD-enabled workaround without ever being detected by the organization. In that case, when he reassesses the situation and determines that *the need for the workaround does not exist anymore*, he will simply stop using his personal device and start using the device recommended by the organization.

Conditions C: When the workaround is validated (sometimes up to the organizational level)

As previously mentioned, management and the IT department may tolerate for a while BYOD-enabled workarounds because they perceive an efficiency gain without giving rise to compliance issues. Seeing this informal acceptance, other employees may start enacting these workarounds gradually creating *a certain mass of adopters*. At that point, maintenance becomes difficult for individual employees and the organization needs to step in. Accepting to take responsibility for the BYOD-enabled workaround is a key step in the *validation and the legitimization of the BYOD-enabled practice* (Chua et al., 2014). The informal tolerance may even transform into formal policies, norms and permission to use personal devices for work purposes (Koeffer et al., 2015). More importantly, Koeffer at al. found that this permission directly impacts individual IT innovation behavior. Therefore, when *permission and formal* *policies* are introduced to control and to protect the BYOD-enabled practice, individual employees become even more innovative with the use of their personal devices for work (Koeffer et al., 2015).

Workarounds are generally associated with negative consequences, but they may also have a positive effect on the underlying business process (Alter, 2014). From this perspective, it is a form of bottom-up innovation, sometimes restricted, sometimes enabled, by organizational structures. The duality of structure implies that the organization changes individual behavior, but employees can also change these structures by re-appropriating and engaging with these organizational practices (Mokosch et al., 2015). Polices, existing technology, tasks and authority will all have a structuring effect on employees' enactment of the BYOD-enabled workaround.

Table 1 summarizes the conditions regulating the proposed conceptual model.

	Conditions A	**Conditions B**	**Conditions C**
Pre-conditions	• Need for a different device to enact an IS-enabled practice. • Inability of the organization to address the need.		
Organizational conditions	• Conducive organizational environment (policies, norms, control, security culture, culture of innovativeness with IT).	• Cannot allow the workaround. • Do not recognize the need. • Tolerate as long as efficiency gain and security compliance.	• Presence of a mass of adopters • Validation and legitimization (permission, policies, control)
Individual conditions	• Personal innovativeness. • Knowledge about the device. • Satisfaction from using the device in private life. • Expected benefits. • Belief that workaround amends a weakness in the business process.	• Misjudged benefits or risks. • Need does not exist anymore.	

Table 1. Conditions regulating the proposed conceptual model

Conclusion

While Alter's theory of workarounds is extremely useful in structuring workarounds, this emergent paper proposes a dynamic explanation of BYOD-enabled workarounds as a first step for addressing an important yet understudied topic in the literature (Azad and King, 2012; Röder et al., 2014a; Röder et al., 2014b). Unlike a framework or classification system (what Gregor calls a Type I theory), Figure 1 aims to explain how and why the BYOD-enabled workarounds are enacted; it is what Gregor (2006) would call a Type II theory. We have now a better understanding of why employers feel that they cannot prevent employees from using a BYOD approach. If a mix of conditions is already in place, there isn't indeed much to do but to embrace the reality. We expect that empirically testing this model based on case studies or on an interpretive field study will result in a clearer picture of the underlying dynamics of BYOD-enabled workarounds, thus providing an initial basis to encourage further research on this topic.

REFERENCES

Alter, S. 2014. "Theory of workarounds," *Communications of the Association for Information Systems* (34:Article 55), pp. 1041-1066.

Anonymous 2013. "Nearly 60% of companies are vulnerable to BYOD risks," *NetworkWorld Asia* (10:3), p. 5.

Azad, B., and King, N. 2012. "Institutionalized computer workaround practices in a Mediterranean country: an examination of two organizations," *European Journal of Information Systems* (21:4), pp. 358-372.

Chua, C., Storey, V., and Chen, L. 2014. "Central IT or Shadow IT? Factors shaping users' decision to go rogue with IT," International Conference on Information Systems (ICIS), Auckland, NZ.

Cidon, A. 2015. "The only way to control BYOD is to embrace it," *Health management technology* (36:4), 2015-Apr, pp. 12-13.

Cook, T., Jaramillo, D., Katz, N., Bodin, B., Cooper, S., Becker, C.H., Smart, R., and Lu, C. 2013. "Mobile innovation applications for the BYOD enterprise user," *IBM Journal of Research and Development* (57:6), pp. 1-10.

French, A.M., Guo, C., and Shim, J. 2014. "Current status, issues, and future of Bring Your Own Device (BYOD)," *Communications of the Association for Information Systems* (35:1), p. 10.

Gregor, S. 2006. "The nature of theory in information systems," *MIS Quarterly* (30:3), pp. 611-642.

Johnson, S. 2013. "Bringing IT out of the shadows," *Network Security* (2013:12), pp. 5-6.

Koeffer, S., Ortbach, K., Junglas, I., Niehaves, B., and Harris, J. 2015. "Innovation Through BYOD? The Influence of IT Consumerization on Individual IT Innovation Behavior," *Business & Information Systems Engineering* (57:6), Dec, pp. 363-375.

Li, N., Mitchell, J.C., and Winsborough, W.H. 2005. "Beyond proof-of-compliance: Security analysis in trust management," *Journal of the ACM* (52:3), pp. 474-514.

Maddox, T. 2015. "CES 2015: The big trends for business," *TechPro Research*. Web. (access date: February 26, 2016, http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/.

Mokosch, G., Klesel, M., and Niehaves, B. 2015. "Putting flesh on the duality of structure: the case of IT consumerization," Americas Conference on Information Systems (AMCIS), Puerto Rico.

Ogie, R. 2016. "Bring Your Own Device: An overview of risk assessment," *Consumer Electronics Magazine, IEEE* (5:1), pp. 114-119.

Orlikowski, W.J. 1996. "Improvising organizational transformation over time: A situated change perspective," *Information Systems Research* (7:1), pp. 63-92.

Ortbach, K. 2015. "Unraveling the Effect of Personal Innovativeness on Bring-Your-Own-Device (BYOD) Intention-The Role of Perceptions Towards Enterprise-Provided and Privately-Owned Technologies," European Conference on Information Systems (ECIS).

Pavlou, P.A., and El Sawy, O.A. 2010. "The "third hand": IT-enabled competitive advantage in turbulence through improvisational capabilities," *Information Systems Research* (21:3), pp. 443-471.

Rivard, S. 2014. "Editor's comments: the ions of theory construction," *MIS Quarterly* (38:2), pp. iii-xiv.

Röder, N., Wiesche, M., and Schermann, M. 2014a. "A situational perspective on workarounds in IT-enabled business processes: A multiple case study," European Conference on Information Systems (ECIS), Tel Aviv, Israel.

Röder, N., Wiesche, M., Schermann, M., and Krcmar, H. 2014b. "Why managers tolerate workarounds–the role of information systems," Americas Conference on Information Systems (AMCIS), Savannah, GA.

Ruighaver, A.B., Maynard, S.B., and Chang, S. 2007. "Organisational security culture: Extending the end-user perspective," *Computers & Security* (26:1), pp. 56-62.

Walters, R. 2013. "Bringing IT out of the shadows," *Network Security* (2013:4), pp. 5-11.

Weeger, A., Wang, X., and Gewald, H. 2015. "IT consumerization: BYOD-program acceptance and its impact on employer attractiveness," *The Journal of Computer Information Systems* (56:1), pp. 1-10.