International Journal of Information Management 43 (2018) 76–84

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users

Paméla Baillette[a], Yves Barlette[b,*], Aurélie Leclercq-Vandelannoitte[c]

[a] Montpellier Research in Management (MRM), University of Perpignan, Via Domitia, 52 Av. Paul Alduy, 66100, Perpignan, France
[b] Montpellier Research in Management (MRM), Member of LabEx Entrepreneurship, Montpellier Business School, 2300 Avenue des Moulins, 34185, Montpellier cedex 4, France
[c] CNRS, LEM (UMR 9221), IESEG School of Management, 3, rue de la digue, 59000, Lille, France

ARTICLE INFO

Keywords:
Reversed IT adoption logic
BYOD
CEOs
Security paradoxes
Personal Mobile tools

ABSTRACT

This research focuses on bring your own device (BYOD), i.e., the use of personal devices (laptops, tablets and smartphones) to fulfil organizational tasks. BYOD provides opportunities, including the possibility of working differently, for both CEOs and end users. However, BYOD involves high organizational and end user security risks. What are the benefits and risks for CEOs and end users of the reversed adoption logic of BYOD, and how can BYOD-related security paradoxes be overcome? A theoretical analysis is conducted with regard to the concept of the "*reversed IT adoption logic*" vs. the traditional IT adoption logic. This analysis highlights the security paradoxes linked to this reversed IT adoption and proposes means to overcome these paradoxes. If BYOD entails many opportunities, then it requires information security management to balance the induced risks for CEOs and users.

1. Introduction

BYOD involves the use in a professional context of privately owned consumer *devices*, such as laptops, tablets and smartphones (Boughzala, 2016; Hovav & Putri, 2016; Magruder, Lewis, Burks, & Smolinski, 2015; Meske, Stieglitz, Brockmann, & Ross, 2017; Singh, 2012; Weeger, Wang, & Gewald, 2016). The worldwide BYOD market is rapidly growing: This market was worth nearly $113 billion in 2016 and could represent $318 billion by 2022, according to Research and Markets[1] (2017). BYOD is a phenomenon that presently affects most organizations and is part of a growing IT "consumerization" trend, i.e., the adoption in a work context of consumer market technologies (De Kok, Lubbers, & Helms, 2015; Harris, Ives, & Junglas, 2012; Jarrahi, Crowston, Bondar, & Katzy, 2017). IT consumerization reverses the traditional IT adoption logic, analyzed as a top-down process (Köffer, Ortbach, Junglas, Niehaves, & Harris, 2015), and generates a bottom-up trend, defined as the "*reversed IT adoption logic*" (2015b, Leclercq-Vandelannoitte & Bertin, 2018; Leclercq-Vandelannoitte, 2015a). As explained by Andriole (2012), p.51), the life cycle of technology adoption has reversed, in that "*employees bring experience with consumer technologies in the workplace and pressure their companies to adopt new technologies*". BYOD is of particular interest to a variety of organizations and employers, in that it is said to increase employees' motivation, satisfaction, innovation, levels of comfort, and performance (Gens, Levitas, & Segal, 2011; Harris et al., 2012), offering new productivity gains at the organizational level (Disterer & Kleiner, 2013; Köffer, Ortbach & Niehaves, 2014) while reducing technological costs (Singh, 2012). In particular, BYOD seems particularly promising for CEOs, as it appears to be a powerful cost-saving lever and productivity lever (Baillette & Barlette, 2018). Thus, CEOs often allow their employees to use their personal tools (devices and applications) to enjoy many benefits for their companies (Baillette & Barlette, 2018).

Via the reversed IT adoption logic, BYOD thus not only offers several opportunities but also raises technical, security and legal problems (Harris et al., 2012; Disterer & Kleiner, 2013); in particular, BYOD entails actual risks for the security of the information stored in users' mobile tools and for the organizational information managed by CEOs (Ding et al., 2014). In part, the reason is a lack of integrated protection for these tools, which are put on the market every day. Hence, user risky behaviors – which are more likely to exploit the potential of these tools than to prevent risks – must be emphasized (Awad & Krishnan, 2006; Dinev & Hart, 2006; Keith, Thompson, Hale, Lowry, & Greer, 2013; Sutanto, Palme, Tan, & Phang, 2013). When CEOs are entrepreneurs, other specific risks appear: entrepreneurs are innovative

* Corresponding author.
E-mail addresses: pamela.baillette@univ-perp.fr (P. Baillette), y.barlette@montpellier-bs.com (Y. Barlette), a.leclercq@ieseg.fr (A. Leclercq-Vandelannoitte).
[1] https://www.researchandmarkets.com/research/7q48z2/global_enterprise.

https://doi.org/10.1016/j.ijinfomgt.2018.07.007
Received 5 June 2018; Received in revised form 16 July 2018; Accepted 16 July 2018

and tend to perceive business situations in a positive manner (Dai, Ivanov, & Cole, 2017; Dushnitsky, 2010; Palich & Bagby, 1995). The issues raised by BYOD and the reversed IT adoption logic are thus particularly acute and relevant, all the more so since the modern economy features massive increases in the number of self-employed workers, freelancers, small to medium-sized enterprises (SMEs) and entrepreneurs (Bohas, Fabbri, Laniray, & de Vaujany, 2018).

However, although literature on IT consumerization is important, research analyzing the specific risks vs. benefits of the reversed IT adoption logic is scarce and remains a challenge, specifically regarding the paradoxes generated (Becker, von Brocke, Heddier, & Seidel, 2015).

To fill this gap on this topic, the research questions addressed in this paper are as follows: What are the benefits and risks for CEOs and end users of the reversed IT adoption logic of BYOD, and how can BYOD-related security paradoxes be overcome? To answer these questions, we develop a theoretical analysis based on a literature review related to the concept of the *reversed IT adoption logic* (2015b, Leclercq-Vandelannoitte & Bertin, 2018; Leclercq-Vandelannoitte, 2015a) vs. the *traditional IT adoption logic*. Our analysis then highlights the security paradoxes linked to this reversed IT adoption among CEOs and end users and discusses its implications for information security management. This research encompasses both theoretical and practical interests. From a practical perspective, it is necessary for CEOs, and specifically for entrepreneurs who are often innovative and inclined to consider events in a positive manner, to take into account not only the benefits but also the risks of the IT adoption logic. Our main practical objective is therefore to raise the awareness of CEOs regarding the BYOD phenomenon and to provide suggestions to enjoy the related benefits while reducing the risks stemming from this reversed IT adoption. From a theoretical perspective, we intend to extend our understanding of reversed IT adoption logic in the organizational context. Another theoretical contribution is the analysis and discussion of the security paradoxes associated with this logic.

This paper is structured as follows: In the second section, we specify the links between BYOD and the reversed IT adoption logic. The third section highlights the BYOD-related security paradoxes and offers suggestions to overcome the involved risks. Section four highlights the theoretical and managerial contributions, identifies some limits of this work and offers avenues for future research.

2. BYOD and the reversed IT adoption logic

IT adoption has generated a great deal of research by sociologists, cognitive scientists, communication specialists and economists. Many models coexist, at both the individual and organizational levels. In this paper, we highlight the evolution of the adoption practices generated by BYOD; then, we explain the benefits of these adoption practices for organizations and CEOs, on the one hand, and for end users, on the other hand.

2.1. BYOD in terms of reversed IT adoption vs. the classical foundations of IT adoption

After explaining the classical foundations of IT adoption, this paper focuses on a specific concept, especially when considering the scarcity and novelty of current research: the *reversed IT adoption logic* (2015b, Andriole, 2012; Leclercq-Vandelannoitte & Bertin, 2018; Leclercq-Vandelannoitte, 2015a).

2.1.1. The traditional IT adoption logic

Technological innovation has traditionally been viewed and analyzed as a top-down process: This innovation is designed and initiated in organizations by IT managers and IT specialists. In this context, IT adoption, as part of the appropriation process, is part of a mechanism by which the organization decides to choose and acquire a technology, to propose it, or even to impose it with regard to organizational actors (Jokonya, 2016; Venkatesh, Morris, Davis, & Davis, 2003). In organizations, the investment decision, constrained by the stakes involved and the necessities of return on investment, is generally planned and organized by CEOs. However, the decision is not always finalized and rational (Willcocks, 2013). Choice and acquisition particularly depend on an "organizing vision", as developed by Swanson and Ramiller (1997), 2004). Inspired by the neo-institutionalist trend, these authors consider that the decision to adopt a technology or not is made according to a representation or idea focused on the purpose of IT and its implementation, the conditions necessary to achieve added value by using this IT, or the organizational changes involved, considering that the representation of the meaning given to technology, and its use, strongly structures the decisions made around its implementation.

The organizational benefits of IT adoption depend on the acceptance and appropriation of the resulting changes in work practices by the organization's members (Orlikowski & Hofman, 1997). Research on this topic involves widely used theories in information systems such as diffusion theory (Rogers, 1962), acceptance models of technologies such as the technology acceptance model (TAM) (Davis, 1989) and the unified theory of acceptance and use of technology (UTAUT and UTAUT2) (Venkatesh, Thong, & Xu, 2012; Dwivedi, Rana, Jeyaraj, Clement, & Williams, 2017; Alalwan, Dwivedi, & Rana, 2017; Dwivedi, Rana, Janssen et al., 2017; Martins, Oliveira, & Popovič, 2014; Mortenson & Vidgen, 2016; Oliveira, Faria, Thomas, & Popovič, 2014; Rana, Dwivedi, Williams, & Weerakkody, 2016; Rana, Dwivedi, Lal, Williams, & Clement, 2017; Venkatesh et al., 2003; Williams, Rana, & Dwivedi, 2015), or strategic alignment models (Henderson & Venkatraman, 1993; Tanriverdi, Rai, & Venkatraman, 2010). As IT adoption is managed at the organizational level, particularly by CEOs in conjunction with IT specialists, end users are "requested" to adopt and cope with tools to work.

For mobile devices, this traditional approach to IT adoption is illustrated by choose your own device (CYOD), where CEOs select and provide end users with professional mobile devices (Brodin, 2016; De Kok et al., 2015), whether laptops, tablets or, increasingly, smartphones. In this case, the organization owns the devices, which helps limit the risks associated with the security of the information stored in these tools, particularly because it is possible to rigorously monitor the precise range of the mobile tools offered to end users, which may also contain preinstalled applications and elaborate security features (standby passwords, antivirus, etc.). However, these devices create dual-equipment and practical constraints for employees. Moreover, the traditional approach involves financial and management constraints for organizations and CEOs: investment in tools, security, the management of tool allocation and maintenance, etc. These constraints are exacerbated by the proliferation of personal devices operated by end users in a professional context and by the more or less explicit encouragement given by some organizations to their employees to use their own equipment (Leclercq-Vandelannoitte, 2015a).

2.1.2. The reversed IT adoption logic

The phenomenon of mobile technology consumerization is increasingly growing in organizations (De Kok et al., 2015; Harris et al., 2012; Jarrahi et al., 2017; Weeger et al., 2016). Certain technological innovations tend to impose themselves on the mainstream market before being disseminated in organizations. IT consumerization is defined as the adoption of consumer applications and devices in the workplace (Harris et al., 2012), and BYOD, i.e., the use of personal mobile tools in a professional context (Boughzala, 2016; Hovav & Putri, 2016; Magruder et al., 2015; Singh, 2012; Weeger et al., 2016), is precisely an illustration of this consumerization of IT (Meske et al., 2017), leading to the reversed adoption logic concept (2015b, Leclercq-Vandelannoitte, 2015a). In this logic (see Fig. 1) and given the evolution of mobile devices and software, the use of personal tools has become increasingly autonomous due to the ease of use of these devices and the benefits of their numerous innovative applications (Cook et al., 2013; Köffer et al.,