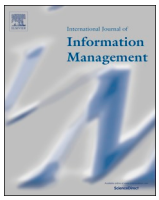
Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

International Journal of Information Management 56 (2021) 102212

Contents lists available at ScienceDirect

International Journal of Information Management

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



Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies

Yves Barlette[a,*], Annabelle Jaouen[a], Paméla Baillette[b]

[a] Montpellier Business School, 2300 Avenue des Moulins, 34185, Montpellier cedex 4, France
[b] University of Bordeaux, IRGO Research Center, 35 Avenue Abadie, CS51412, 33072, Bordeaux cedex, France

ARTICLE INFO

Keywords:
BYOD
Reversed IT adoption
CMUA
Coping
Emotion-focused

ABSTRACT

The adoption of Bring Your Own Device (BYOD), initiated by employees, refers to the provision and use of personal mobile devices and applications for both private and business purposes. This bottom-up phenomenon, not initiated by managers, corresponds to a reversed IT adoption logic that simultaneously entails business opportunities and threats. Managers are thus confronted with this unchosen BYOD usage by employees and consequently adopt different coping strategies. This research aims to investigate the adaptation strategies embraced by managers to cope with the BYOD phenomenon. To this end, we operationalized the coping model of user adaptation (CMUA) in the organizational decision-making context to conduct a survey addressing 337 top managers. Our main results indicate that the impact of the CMUA constructs varies according to the period (pre- or post-implementation). The coping strategies differ between those who have already implemented measures to regulate BYOD usage and those who have not. We contribute to theory by integrating the perception of BYOD-related opportunities and threats and by shedding light on the decisional processes in the adoption of coping strategies. The managerial contributions of this research correspond to the improved protection of corporate information and the maximization of BYOD-related benefits.

1. Introduction

The BYOD phenomenon, i.e., Bring Your Own Device, refers to the provision and use of personal mobile devices and applications by employees for both private and business purposes (Cho & Ip, 2018; Hovav & Putri, 2016; Middleton, Scheepers, & Tuunainen, 2014). As opposed to the classic top-down adoption usually imposed by top management, the BYOD phenomenon is considered to be a disruptive event that is often a bottom-up process, in other words, reversed IT adoption starting with employees (Leclercq-Vandelannoitte & Bertin, 2018).

Since its early period 10–15 years ago, BYOD has undergone major changes. The first evolution related to the devices themselves, which were initially limited to mobile phones and laptops and now include smartphones (approximately 90 %), tablets, and connected devices. The second evolution corresponds to the power and increased connectivity of devices: today's smartphones can include up to 10 cores, offering performance similar to low-end laptops. In terms of connectivity, if the speed of Internet connections underwent dramatical acceleration,[1] the range of networks now includes hi-speed Wi-Fi, Bluetooth and NFC.[2] Elaborated applications can operate on personal devices, ranging from emails to critical business applications, such as CRM and ERPs (Ding et al., 2014). In addition, access to cloud-based applications and storage has reinforced even more the variety and sophistication of applications. Operating systems have also evolved from proprietary and often secured solutions (e.g., Blackberry phones) to more open and democratized platforms, such iOS and Android.

However, although all of these evolutions increase significantly the opportunities offered by mobile and connected devices, they also involve higher risks. BYOD opportunities are reflected by recent figures showing that companies favoring BYOD obtain an annual savings of $350 per year per employee (Cisco, 2016). Using portable devices for work tasks can also increase productivity by 34 % (Frost and Sullivan, 2016). BYOD threats relate to additional security breaches, mainly data leakage and malware infiltration. For example, in 2017, employeeowned devices were culpable in 51 % of corporate data breaches (AT and T, 2017). Such breaches not only endanger the firm itself but also allow access to companies' external partners through the Internet or other digital exchanges, dramatically increasing their vulnerability to

* Corresponding author.
E-mail addresses: y.barlette@montpellier-bs.com (Y. Barlette), a.jaouen@montpellier-bs.com (A. Jaouen), pamela.baillette@u-bordeaux.fr (P. Baillette).

[1] Between 3G and 5G, speed has been multiplied by 1,000 − 10,000.
[2] Near Field Communication

https://doi.org/10.1016/j.ijinfomgt.2020.102212
Received 28 April 2020; Received in revised form 4 August 2020; Accepted 4 August 2020
Available online 11 September 2020

cyber-attacks (Lowry, Dinev, & Willison, 2017; McLeod & Dolezel, 2018; Sokolova, Perez, & Lemercier, 2017). However, despite laws and regulations, there is a lack of effective security measures regarding the specificity of BYOD: for instance, only 40 % of employees are subject to regulations regarding personal device usage (Kemper, 2018).

These figures emphasize the importance of this phenomenon, all the more so because BYOD is increasingly used in businesses and often spontaneously introduced by employees without any regulations to prevent security issues (Weeger et al., 2020). Employees have an individualistic perception of BYOD opportunities, and their security concerns are mainly focused on privacy issues. However, managers go beyond these individual issues and must consider the organizational impacts of BYOD. Unfortunately, managers do not necessarily perceive the actual opportunities and threats that "rogue" adoption of BYOD represents for their organizations. Since they can barely prohibit its usage within the firm (Baillette, Barlette, & Leclercq-Vandelannoitte, 2018), especially because the company does not own the devices, they often make reactive decisions according to their own subjective perceptions of BYOD opportunities and threats (Hu, Dinev, Hart, & Cooke, 2012; Puhakainen & Siponen, 2010).

The previous research regarding the perception of BYOD-related opportunities has mainly focused on individuals and has highlighted a set of factors determining the adoption of mobile tools by employees (Hoehle, Zhang, & Venkatesh, 2015; Middleton et al., 2014; Weeger, Wang, & Gewald, 2016). In terms of BYOD-related threats, the literature has addressed issues related to employee privacy (Garba Bello, Murray, & Armarego, 2017; Pentina, Zhang, Bata, & Chen, 2016) and employee compliance with information security (ISS) policies (Cho & Ip, 2018; Palanisamy, Norman, & Mat Kiah, 2020). Academic research studying how managers cope address bottom-up adoption of BYOD and the types of decisions that they consequently make has been scarce (Baillette et al., 2018; Baker & Singh, 2019; Leclercq-Vandelannoitte & Bertin, 2018; Tu & Yuan, 2015).

Therefore, obtaining insights into managers' coping strategies is important to better understand how they can address and regulate BYOD usage, i.e., maximizing the benefits and mitigating the threats. This understanding will also enable managers to better administer and adapt policy and regulatory measures. This article thus investigates the following research question: *what adaptation strategies do managers adopt to cope with the BYOD phenomenon?* This implies the investigation of (a) managers' perception of BYOD opportunities and threats; and (b) the coping strategies they decide to adopt accordingly.

We use the coping model of user adaptation (CMUA, Beaudry & Pinsonneault, 2005, 2010), based on Lazarus' coping theory (1966). This model allows us to investigate the determinants of managers' "*behaviors that occur before, during, and after the implementation of a new IT*" (Beaudry & Pinsonneault, 2005, p. 2) and their resulting coping strategies. It also fits individual, as well as organizational, contexts (Tobler, Colvin, & Rawlins, 2017). However, the research has seldom used this model, with mostly qualitative methods (Beaudry & Pinsonneault, 2010; Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011; Tobler et al., 2017). In this article, we test the CMUA framework through a quantitative study of 337 managers.

Our article contributes to the academic literature in IS by offering insights into managers' perceptions of BYOD adoption by employees, encompassing both opportunities and threats and the decisions stemming from these perceptions. Four types of coping strategies are investigated and discussed, hereby extending the literature on IT adoption, reversed IT adoption, and information security. An important managerial implication of this paper is the identification of a "stop-and-start" process, reflecting evolution of managers' perceptions before and after addressing BYOD usage in their companies.

The remainder of this paper is organized as follows. Section 2 discusses the theoretical background of BYOD and the CMUA. In Section 3, we present the research model and develop hypotheses. Section 4 describes the research methods that we use to determine the decisions stemming from managers' perceptions of BYOD implementation and set forth how we complement the CMUA framework. The results are presented in Section 5. This analysis is followed in Section 6 by a discussion of the findings; the contributions to theory, practice and policies; and the study's limitations and suggestions for future research.

2. Theoretical background

Researchers and practitioners agree that BYOD is illustrative of the IT consumerization trend (Jarrahi, Crowston, Bondar, & Katzy, 2017; Koch, Yan, & Curry, 2019; Köffer, Ortbach, Junglas, Niehaves, & Harris, 2015; Weeger et al., 2020; Zhang, Mouritsen, & Miller, 2019). By reversing the traditional IT adoption logic (Baillette et al., 2018), BYOD creates a disruption in adoption practices (Köffer et al., 2015; Leclercq-Vandelannoitte & Bertin, 2018; Steelman, Lacity, & Sabherwal, 2016) and requires new managerial decisions and behaviors (Koch et al., 2019). One challenge for researchers is shedding light on this phenomenon. To do so, in the first subsection, we present the theoretical underpinnings of BYOD opportunities and threats. We then detail the possible interventions (at technological or behavioral levels) and focus on the importance of adopting suitable managerial behaviors to address the organizational issues involved in BYOD usage. In the second subsection, we introduce the CMUA framework, which allows us to investigate the behaviors (coping strategies) resulting from managers' appraisals of opportunities and threats.

2.1. Opportunities and threats of BYOD

2.1.1. BYOD and its related opportunities

Since it is usually initiated by employees themselves, BYOD has been shown to increase their autonomy, motivation, satisfaction, innovation and performance (Harris, Ives, & Junglas, 2012; Koch et al., 2014). This employee-chosen adoption leads to easier assimilation and more efficient use, and employees can creatively adapt their own tools and reinterpret workplace tasks (Schmitz, Teng, & Webb, 2016). BYOD improves the quality of employee interactions, helps to recognize employees' achievements and encourages peer-to-peer employee recognition, in turn favoring employee retention.

Organizations can also benefit from numerous tool-embedded innovations (Cook et al., 2013; Köffer et al., 2015; Zhang et al., 2019), such as the use of social media, which has proved its efficiency regarding firm performance (Chatterjee & Kar, 2020). For example, employees can use personal apps that initiate new ways to serve the firm's objectives in terms of work performance (Doargajudhur & Dell, 2019; Junglas, Goel, Ives, & Harris, 2019; Leclercq-Vandelannoitte & Bertin, 2018). By doing so, BYOD enables employees to initiate changes that lead to improving and rethinking some organizational processes (Koch et al., 2019; Köffer et al., 2015). Because these devices are the employees' property, BYOD reduces organizational costs in terms of tool funding or management (Baillette et al., 2018). Furthermore, some emergency situations, such as those related to pandemics (such as Covid-19), promote the use of BYOD when professional devices are no longer accessible (Davison, 2020; Papagiannidis, Harris, & Morton, 2020; Richter, 2020). BYOD becomes a necessary practice because it enables employees to continue to communicate and work despite social distancing and new working conditions.

Finally, at an organizational level, BYOD opportunities correspond to cost savings (Benlian & Hess, 2011; Steelman et al., 2016); productivity gains (Leclercq-Vandelannoitte, 2015a; Morrow, 2012; Singh, 2012; Steelman et al., 2016); increased innovation, mainly in terms of business process improvement (Aydiner, Tatoglu, Bayraktar, & Zaim, 2019; Law & Ngai, 2007; Zhou, Lu, & Wang, 2010), and performance expectancy (Moore & Benbasat, 1991; Venkatesh, Morris, Davis, & Davis, 2003).

2.1.2. BYOD and its related threats

BYOD and mobile applications involve security issues not only threatening their adoption and diffusion (Balapour, Nikkhah, & Sabherwal, 2020) but also increasing the threats to organizational data, for several reasons. First, hyperconnected BYOD tools increase the complexity of network protection because they can connect to several types of networks (cellular networks, Wi-Fi, Bluetooth and NFC), (Breitinger, Tully-Doyle, & Hassenfeldt, 2020; McLeod & Dolezel, 2018; Palanisamy et al., 2020) and to cloud computing resources, thereby increasing the risks (Ding et al., 2014; Gupta, Seetharaman, & Raj, 2013; Lian, Yen, & Wang, 2014; Morrow, 2012; Sultan, 2014). Smartphones and tablets are increasingly connected to applications, storage or other digital services, resulting in greater risks (Mustafa & Kar, 2019). In addition, cloud-based resources are often located in public clouds, which are more prone to malware, viruses (Ali, Shrestha, Soar, & Fosso Wamba, 2018) and unauthorized access by cloud administrators (Kaw et al., 2019). More recently, the explosion of IoT and connected devices brought to work by employees has worsened the risks (Kaw et al., 2019; Tanenbaum, 2016) because connections and even devices themselves are often poorly secured.

Second, the use of personal tools for work also increases the risk that devices will be lost or stolen (Jones & Chin, 2015; Nokia, 2019; Tu, Turel, Yuan, & Archer, 2015), endangering organizational data (Baillette et al., 2018). Third, smartphones have become a lucrative target for cybercriminals (Chatterjee, Kar, Dwivedi, & Kizgin, 2019; Checkpoint, 2020), and corporate data can be corrupted by attacks through hacked or malware-infected smartphones. Fourth, since employees own the devices, their run greater risks when using BYOD than they do when using corporate tools (Hovav & Putri, 2016) or computers (McGill & Thompson, 2017; Thompson et al., 2017). Moreover, it is more difficult to monitor their usage and compliance with organizational policies and regulations (Hovav & Putri, 2016). The risk is even greater for younger generations, mainly digital natives, because they tend to only see the potential benefits of BYOD and neglect the risks to themselves and their institutions (Baillette & Barlette, 2020; Weeger et al., 2020). Employees' priority is mainly to protect their private information (Mustafa & Kar, 2019), and they might less care about their organizational data since they are less "personally relevant" (Barlette & Jaouen, 2019). Moreover, privacy-protective controls and settings on mobile devices are difficult to find and activate, and employees can be reluctant to enact privacy-protective behaviors (Crossler & Bélanger, 2019).

Therefore, seen from a manager's perspective, BYOD can harm the organization's information system security and lead to failure. Failure can correspond to information failure (compromised data security), functional failure and system failure and can eventually lead to service failure from companies (Mustafa, Kar, & Janssen, 2020).

2.1.3. How can managers address BYOD opportunities and threats?

A manager mainly considers the BYOD-related perceived opportunities at the organizational level. Tobler et al. (2017) showed that people in power usually focus on problems and adapt technologies to their own ways of working. Hence, to reap these benefits, managers can guide the required changes in business processes. Managers can also facilitate change and innovation by transforming their management practices (Damanpour, 2014; Leclercq-Vandelannoitte, 2015b). They can also simply be supportive, i.e., provide top management support (TMS, Boonstra, 2013) in seizing the benefits of BYOD usage by showing their involvement, being participative and providing resources when necessary (Liu, Wang, & Chua, 2015).

To mitigate the risks stemming from BYOD usage by employees, many IT-based possibilities exist, such as reinforced passwords, system updates and antivirus software. More specific to BYOD, mobile device management (MDM) software can be implemented on the personal tools of employees to improve the security of organizational data. Employees willing to connect to the corporate network can also be granted a restricted access to a "guest" network. Finally, new software solutions, such as cloud access security brokers (CASBs), can provide security for remote workers who are increasingly accessing applications and data in the cloud (Gartner, 2019), especially when working with their personal devices from home (Bitglass, 2020; Papagiannidis et al., 2020). However, better protective technologies are not sufficient (Williams, Wynn, Madupalli, Karahanna, & Dunkan, 2014) to efficiently mitigate BYOD-related security issues; protective behaviors and attitudes are also important (Aurigemma & Mattson, 2019; Balapour et al., 2020). Some security measures can directly affect the company's management and thus require organizational reflection (Brodin, 2016) and management's decision making (Jeong, Lee, & Lim, 2019). Hence, managers can also intervene in corporate culture to trigger changes in attitudes toward more compliant and secure employee behaviors. These changes can be initiated by teaching individuals how to improve their security behaviors (Balapour et al., 2020; White, Ekin, & Visinescu, 2017) and awareness-raising campaigns. Employees can be also driven to sign a BYOD-specific charter (Harrington, 1996), specifying the particular risks arising from the use of personal mobile tools, stating responsibilities and explaining what to do in case of device loss, theft or breakdown, for example. Regarding opportunities, to mitigate threats, previous research has unscored the essential impact of TMS on information security behaviors (Barlette & Jaouen, 2019; Herath, Herath, & D'Arcy, 2020; Hu et al., 2012; Puhakainen & Siponen, 2010).

Moreover, Baillette and Barlette (2018) highlighted a twofold security paradox for managers generated by BYOD. The authors show that the perception of BYOD opportunities, i.e., the numerous benefits of BYOD via reversed adoption, outweighs the threats involved. The authors argue that managers overlook BYOD ISS-related issues through either a misperception of the risks or the erroneous feeling that their company is sufficiently protected. Hence, despite a strong concern over ISS, managers may primarily consider the advantages of BYOD without necessarily implementing the required protective actions.

Therefore, the necessity for managers to address BYOD-related opportunities and threats deserves more attention. However, there has been a lack of research about opportunity appraisal and its consequences for behaviors, mainly regarding managers (Baillette et al., 2018). Academic research has also been scarce about threat appraisal and how managers can address information security threats. The previous literature has repeatedly examined ISS-related employee behaviors, including adoption by employees of more secure behaviors, such as antivirus updates, backups (Boss, Galletta, Lowry, Moody, & Polak, 2015) or behaviors related to compliance with ISS policies (D'Arcy & Teh, 2020; Karjalainen, Sarker, & Siponen, 2019; Moody, Siponen, & Pahnila, 2018; Yazdanmehr & Wang, 2016) including theories such as deterrence theory (Xu, Lu, & Hsu, 2020). The behavioral research has integrated threat appraisal as a particularly influencing construct to consider. For instance, threat appraisal has been included as a building block in technology threat avoidance theory (TTAT, Liang & Xue, 2010), the health belief model (HBM, Ng, Kankanhalli, & Xu, 2009) and protection motivation theory (PMT, Rogers, 1983; Crossler, Andoh-Baidoo, & Menard, 2019; Wall & Warkentin, 2020). Business managers are the ultimate decision makers in resource allocation in ISS (Menon & Siponen, 2020). In addition, their decisions are very specific because they are primarily based on preventing loss, the best outcome being that "nothing happens" (Menon & Siponen, 2020). However, the ISS literature has rarely focused on manager behavior (Berry & Berry, 2018; Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016) and on their important role in developing and implementing protective measures, regulations or an ISS culture (Barlette, Gundolf, & Jaouen, 2017; Dojkovski, Lichtenstein, & Warren, 2007; Feng, Zhu, Wang, & Liang, 2019; Indihar Štemberger, Manfreda, & Kovačič, 2011).

Hence, while BYOD entails crucial issues in terms of decision-making to address or not the related opportunities or threats, the interest of the academic research remains recent and has mainly focused on theoretical approaches (Leclercq-Vandelannoitte & Bertin, 2018).

Hence, more empirical studies are required to explore how managers can address BYOD adoption by employees (Baillette et al., 2018). The CMUA constitutes a relevant theoretical framework to investigate managers' behaviors related to the perception of opportunities and threats when they become aware that BYOD has been introduced in their company by employees.

2.2. The CMUA framework

Beaudry and Pinsonneault (2005) based their coping model of user adaptation (CMUA) on Lazarus' (1966, 2000) coping theory from the psychology literature. Coping theory describes the process by which individuals cope with disruptive events in their environment such as the introduction of a new IT (Fang, Benamati, & Lederer, 2011a; Fang, Benamati, & Lederer, 2011b). Coping corresponds to "*the cognitive and behavioral efforts exerted to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person*" (Lazarus & Folkman, 1984, p. 141). Internal demands relate to personal desires or obligations (e.g., need for achievement), and external demands are imposed by the external environment (e.g., social pressures). Such demands can be considered *disruptive events* if they exceed one's resources to manage them (Bhattacherjee, Davis, Connolly, & Hikmet, 2018; Elie-Dit-Cosaque & Straub, 2011).

Beaudry and Pinsonneault (2005) adapted the coping theory to investigate behaviors that occur before, during, and after an IT event. The CMUA postulates that the perception of an IT event triggers adaptive behaviors, based on two key subprocesses. The *primary appraisal* consists of assessing the potential consequences and the personal significance of the event, perceived as a threat and/or an opportunity (Folkman, 1992). The *secondary appraisal* corresponds to the evaluation of the coping strategies available that will guide the individual's choice. This choice will depend on the individual's level of perceived control over the situation. Further studies have since confirmed the insights offered by the CMUA (Bhattacherjee et al., 2018; Elie-Dit-Cosaque & Straub, 2011). The CMUA itself is shown in Fig. 1.

To better contextualize the four coping strategies in this research, we define the *individual* of interest as the manager. The *IT event* that we address corresponds to when managers become aware of BYOD usage by employees within the firm. They personally assess the threats and opportunities related to BYOD for their organizations (primary appraisal). The *situation* that we explore consists of the personal decisions of managers to implement organizational measures to address this BYOD usage (coping strategies). The secondary appraisal corresponds to the manager's perceived control over the situation and its organizational outcomes, either to maximize the benefits or to reduce the threats stemming from the usage of BYOD.

2.2.1. Primary appraisal

Primary appraisal begins when an individual becomes aware of the potential consequences of an IT event and assesses its personal and/or professional relevance and importance (Beaudry & Pinsonneault, 2005; Folkman, 1992). For example, individuals may think that a new tool (hardware or software) will improve their efficiency or their ability to interact with others; thus, they may integrate that new hardware or software into their work routines, which may require (self-)training in the use of the new tool. However, this new tool will appear to be a threat to individuals if they feel insufficiently skilled to use it or if its use may endanger their privacy. Most IT events are multifaceted, and an individual may consider them threats, opportunities or both (Beaudry & Pinsonneault, 2005). In the latter case, it is their relative importance that will influence the choice of adaptation efforts to be made (Lazarus & Folkman, 1984). Some elements may influence this assessment such as whether the tool is perceived as concrete or the potential criticality of the consequences of its use. Similarly, the level of 'task-technology fit' or expected performance may result in a negative (if it is low) or positive (if it is high) perception. This primary appraisal leads to a secondary appraisal (Beaudry & Pinsonneault, 2005; Lazarus & Folkman, 1984).

2.2.2. Secondary appraisal and the four coping strategies

The individual's perception of an IT event as beneficial and/or threatening (i.e., primary appraisal) is followed by the evaluation of the available options (i.e., secondary or coping appraisal), which guide the choice of coping strategies. The CMUA identifies four coping strategies (Table 1), reflecting the coping efforts required to reduce the emotional stress resulting from the situation and adapt to this situation (Beaudry & Pinsonneault, 2005, 2010). The choice of strategies is based on the individual's level of perceived behavioral control (low or high).

A high level of perceived control will cause the individual to adopt mainly problem-focused (i.e., active) coping strategies (*benefits maximizing* and *disturbance handling*). Conversely, a low level of perceived control will mainly cause the individual to adopt emotion-focused (i.e., rather passive) coping strategies (*benefits satisficing* and *self-preservation*). Interestingly, while problem-focused strategies (i.e., "active" behaviors) have often been investigated, emotion-focused strategies (i.e., "passive" behaviors) remain under-researched (Liang, Xue, Pinsonneault, & Wu, 2019).

The *benefits maximizing* strategy occurs when managers perceive the IT event (i.e., BYOD usage by employees) as beneficial, and their perceived control over the coping options available is high. In this case, managers feel able to manage the use of BYOD by their employees. Therefore, managers adopt a problem-focused coping strategy, and they aim to maximize the benefits offered by the situation. For example, managers can implement processes to maximize cost reduction, improve their companies' efficiency and foster new ways of working through BYOD.

The *benefits satisficing* strategy corresponds to passively enjoying the benefits of BYOD. In this case, managers perceive BYOD usage as beneficial, and they do not feel any emotional distress, so there is no need to act to restore their psychological balance. Moreover, since

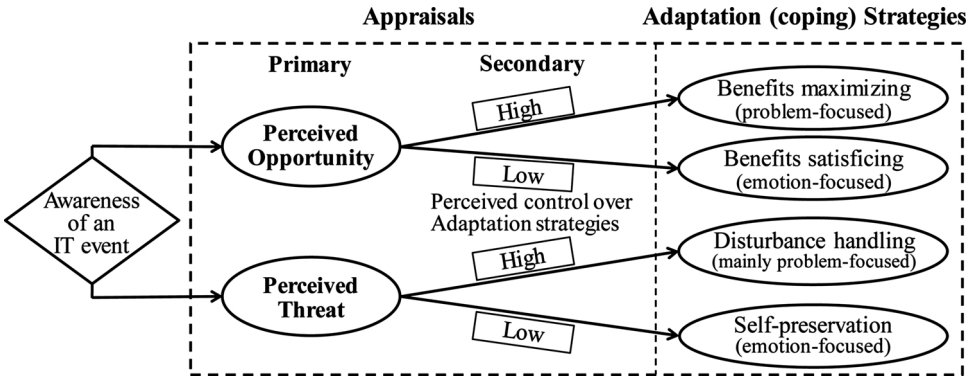


Fig. 1. Original CMUA model (Beaudry & Pinsonneault, 2005).

Table 1
The four coping strategies.
(Adapted from Beaudry & Pinsonneault, 2005).

Control	Low	High
Appraisal	(emotion-focused)	(mainly problem-focused)
Opportunity	Benefits satisficing	Benefits maximizing
Threat	Self-preservation	Disturbance handling

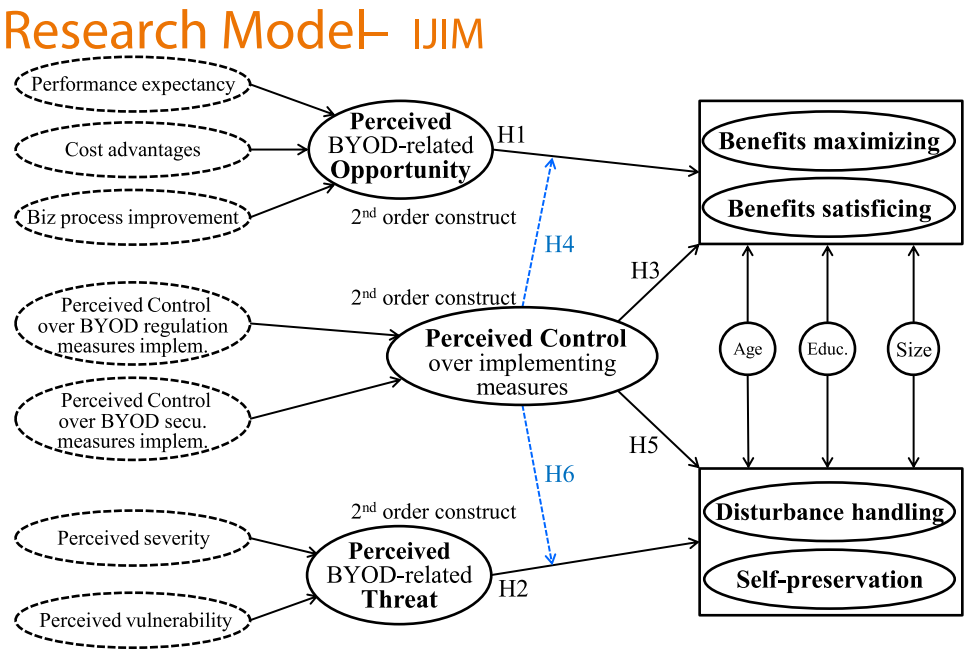


Fig. 2. Enriched CMUA model and hypotheses.

managers' perceived control is low, they will adopt emotion-focused coping strategies, such as being simply satisfied with the use of BYOD by their employees.

The *disturbance handling* strategy occurs when managers perceive BYOD usage as threatening, and they have a high level of perceived behavioral control. In this case, managers feel able to implement protective measures in their companies. Therefore, their coping efforts will be mainly problem focused to mitigate perceived threats and prevent potential negative outcomes.

The *self-preservation* strategy corresponds to the case in which managers perceive BOYD to be a potential threat, but they have limited control. They do not feel able to solve the potential problems, and this situation generates emotional stress. To restore their psychological balance, they adopt emotion-focused coping strategies, such as minimization of consequences, passive acceptance, denial and distancing themselves from the stressful situation.

3. Hypotheses development and research model

At the end of this section, the research model (see Fig. 2[3]) provides an overview of the hypotheses.

3.1. Primary appraisal: opportunity and threat

3.1.1. Effect of perceived opportunity on coping strategies

The previous IS research has shown that perceived benefits have a positive influence on the use of IT devices and applications (Benlian & Hess, 2011; Gupta, Yousaf, & Mishra, 2020; Kim, Jang, & Yang, 2017; Moser, Bruppacher, & Mosler, 2011; Zhou, Jin, Fang, & Vogel, 2015). According to the CMUA, the perceived opportunity of an IT event fosters the adoption of *benefits maximizing* and *benefits satisficing* strategies (Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011).

Top management can perceive BYOD as offering valuable business opportunities and initiate IT-driven changes (Leclercq-Vandelannoitte, 2015b). Managers that perceive the most clearly BYOD-related business opportunities tend to capitalize on employees' initiatives and to regulate and standardize their practices. A high perception of BYOD-related benefits has also been found to favor engagement behavior and satisfaction (Kim, Kim, & Wachter, 2013). Accordingly, we hypothesize the following:

Hypothesis 1a-b. The perception of BYOD usage as an opportunity will positively influence the manager's adoption of the (a) benefits maximizing strategy and (b) benefits satisficing strategy.

3.1.2. Effect of perceived threat on coping strategies

As previously underscored (see 2.1.2.), using organizational data through personal devices involves important threats related to cybersecurity and information risks (Ali et al., 2018; Baillette et al., 2018; Mustafa & Kar, 2019). Moreover, the perception of threat related to security is the central construct in the behavioral stream of research on security because it affects user intentions and behaviors (Balapour et al., 2020). The previous IS research showed that IT events perceived as threats (Lee & Larsen, 2009; Vance, Siponen, & Pahnila, 2012) cause managers to adopt more cautious behaviors (Barlette & Jaouen, 2019; Bulgurcu, Cavusoglu, & Benbasat, 2010). In the context of mobile devices, the perception of a threat exerts a positive and significant influence on the intention to implement ISS protections (Gu, Xu, Xu, Zhang, & Ling, 2017; Koohikamali, French, & Kim, 2019; Liu & Varshney, 2020; Tu et al., 2015; Wottrich, van Reijmersdal, & Smit, 2018; Zhou, Kang, Zhang, & Lai, 2016). Therefore, managers will tend to address

[3] Bold: Original CMUA constructs. Dotted constructs: first-order constructs enriching the original CMUA model (see also 4.2). Dotted arrows: moderating effects.

employees' practices, and top management expectations will correspond to problem-focused behavior, i.e., the development of clear IT policies and the implementation of BYOD-related protection measures (Jarrahi et al., 2017; Leclercq-Vandelannoitte, 2015b). However, when a threat is perceived, but managers have limited control, they will adopt more passive and emotion-focused behaviors, i.e., self-preservation strategies (Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011; Jarrahi et al., 2017). Therefore, we propose the following:

Hypothesis 2a-b. Manager's perception of BYOD usage as a threat will positively influence the adoption of the (a) disturbance handling strategy and (b) self-preservation strategy.

3.2. Secondary appraisal: influence of perceived behavioral control

As the initial CMUA model was qualitative, no indication was given about the effect of perceived behavioral control (Beaudry & Pinsonneault, 2005). Consequently, we hypothesized that perceived behavioral control exerts direct and moderating effects on coping behavior.

3.2.1. Perceived control over addressing BYOD opportunities

This variable reflects the level of control perceived by managers over the implementation of organizational measures to benefit from the use of BYOD by employees. According to the CMUA, they can adopt problem-focused and/or emotion-focused coping responses (Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011). When BYOD is perceived as an opportunity, and their perceived control is high, managers will mainly adopt problem-focused strategies to achieve better performance (Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011; Harris et al., 2012), i.e., benefits maximizing strategies.

Conversely, when the behavioral control perceived by managers over the situation is low since no tension emanates from a beneficial situation (Beaudry & Pinsonneault, 2005; Folkman, Lazarus, Gruen, & DeLongis, 1986), they will passively enjoy the advantages of BYOD use by employees, i.e., adopt an emotion-focused coping strategy corresponding to simply being satisfied. Hence, we propose the following:

Hypothesis 3a-b. (direct effect): When a manager appraises a situation as an opportunity, the more perceived control that s/he has over implementing measures to regulate BYOD usage: (a) the more inclined that s/he will be to adopt a benefits maximizing strategy; and (b) the less inclined that s/he will be to adopt a benefits satisficing strategy.

Hypothesis 4a-b. (moderating effect): When a manager appraises a situation as an opportunity, the level of perceived control that s/he has over implementing regulation measures will: (a) positively moderate the relationship between the BYOD-related opportunity and the benefits maximizing strategy; and (b) negatively moderate the relationship between the BYOD-related opportunity and the benefits satisficing strategy.

3.2.2. Perceived control over addressing BYOD threats

When BYOD usage is perceived as a threat, this variable corresponds to the degree to which managers believe they can implement protective measures (Vance et al., 2012). Prior research has found that, when individuals perceive greater threats related to IT, their protection motivation increases (Li et al., 2019; Thompson, McGill, & Wang, 2017) and can result in protective and nonprotective responses (Baillette & Barlette, 2020; Moser et al., 2011). Increased coping efficacy fosters protective responses (i.e., disturbance handling strategy) (Crossler, Bélanger, & Ormond, 2019; Donalds & Osei-Bryson, 2020; Li et al., 2019) and decreases non-protective responses (Moser et al., 2011). Conversely, low levels of perceived control increase nonprotective responses (i.e., self-preservation strategy), aiming to regulate or reduce the emotional distress triggered by the threat appraisal (Beaudry & Pinsonneault, 2005; Folkman et al., 1986; Jex, Bliese, & Buzzell, 2001; Srivastava & Tang, 2015). Consequently, we propose the following:

Hypothesis 5a-b. (direct effect): When a manager appraises BYOD usage as a threat, the more perceived control s/he has over implementing security measures, (a) the more s/he will adopt disturbance handling strategies and (b) the less s/he will adopt self-preservation strategies.

Hypothesis 6a-b. (moderating effect): When a manager appraises BYOD usage as a threat, the level of perceived control s/he has over implementing security measures will (a) positively moderate the relationship between the BYOD-related threat and the disturbance handling strategy and (b) negatively moderates the relationship between the BYOD-related threat and the self-preservation strategy.

The original CMUA in Fig. 1 has been enriched in two stages. The first stage corresponds to adding hypotheses H3 to H6 related to the effect of perceived control on the four coping strategies (Section 3.2). The second stage corresponds to adding seven constructs (dotted in Fig. 2), permitting a quantitative measurement of perceived opportunities and threats (primary appraisal) and perceived control (secondary appraisal). The details of this second step can be found in Section 4.2, which explains the construct operationalization and measures.

4. Research method

4.1. Research design

To investigate the coping strategies adopted by managers resulting from their perceptions of BYOD usage, we conducted a questionnaire-based survey. We used measurement scales borrowed from the previous literature (see 4.3.). The questions were first discussed and adapted to the BYOD context at three professional seminars held by the authors. The questionnaires were then pretested in face-to-face exchanges with managers (N = 17). Based on their feedback, through six rounds, the authors ensured the understandability and readability of the questions, mostly by removing redundancies. This process led to the final questionnaire (see Appendix A). The questionnaire was managed using the Qualtrics web-based software platform. In the questionnaire introduction, a text presented the objectives of the survey and defined the main terms (information security, personal device, BYOD, etc.). Participation in the survey was voluntary, and the authors clearly assured respondents that their responses would be treated anonymously and confidentially. We added a question to check whether managers intended to implement or had already implemented BYOD measures to address BYOD usage in their companies (Meissonier & Houzé, 2010). Although the question of period (pre- or post-implementation) is important in the MIS literature (Beaudry & Pinsonneault, 2005; Karahanna, Straub, & Chervany, 1999; Marler, Fisher, & Ke, 2009; Taylor & Todd, 1995; Thompson, Compeau, & Higgins, 2006; Veiga, Keupp, Floyd, & Kellermanns, 2014), it does not address the issue of BYOD during these two periods. For this purpose, two slightly different sub-versions of the questionnaire were created, using the past or future tense depending on the actual or planned implementation of measures framing BYOD usage.

The questionnaire administration was outsourced to a panel company and conducted during May 2018. We chose this company because our previous collaborations were satisfying due to the company's rigor. It has a specific division specializing in academic, quantitative and qualitative studies Hence, panel members are used to respond to scholarly questionnaires. It also uses specific methods of online data collection (CAWI in our case) and meets the standards of qualification criteria and quotas. Our criteria corresponded to the respondents' range of ages, and positions (CEOs, top managers or executive and managers in charge of their own service/department/business units, with at least one employee to manage, with hierarchical responsibility). The

respondents had to be in positions and active (non-retired) and not prohibited from BYOD usage.

Our criteria for questionnaire rejection were based on several elements. First, we removed incomplete and invalid responses. Second, all questionnaires with excessively short duration were removed because respondents may have not read and carefully answered our questions. Third we used the respondents' IP addresses to control for duplicate submissions and to check if more than one manager had responded, for a specific location. A total of 384 responses were collected, and after applying our rejection criteria, 337 usable responses were retained.

We ensured the sample size sufficiency using the G*Power tool (Faul, Erdfelder, Buchner, & Lang, 2009) via *a priori* and *post-hoc* power analyses. For that purpose, we adopted a lower bound R^2 value of 0.10, a statistical power of 95 % and three predictors (benefits maximizing, benefits satisficing, disturbance handling and self-preservation constructs have the highest numbers of predictors). The *a priori* G*Power results indicated that a minimal sample size of 143 was required. In addition, the post-hoc G*Power results for a lower bound R^2 of 0.10, a sample size of 143, and three predictors showed that the statistical power was 0.95. These results exceed Cohen's (1988) recommendations and support the sufficiency of our sample size.

4.2. Construct operationalization and measures

The CMUA is conceptually derived from the "coping" theory (Lazarus, 1966). However, this theory is "*mute regarding what elements of a disruption are used in primary appraisal*" (Beaudry & Pinsonneault, 2005, p. 498). Therefore, to assess this primary appraisal, that is, managers' perceptions of opportunities and threats related to BYOD usage by employees, we complemented the CMUA by adding constructs borrowed from the previous research.

To render our model more parsimonious and easier to apprehend (Hair, Sarstedt, Ringle, & Gudergan, 2018, p. 40), we created two higher-order[4] constructs (Hair, Hult, Ringle, & Sarstedt, 2017). Higher-order constructs allow for overcoming the jangle fallacy, and they are better predictors of broadly defined behaviors, (Hair et al., 2018).

Hence, *BYOD-related opportunity* and *BYOD-related threat* were operationalized as two higher-order constructs composed of several lower-order reflective constructs. We used the same logic to assess the secondary appraisal, based on *perceived behavioral control*.

These higher-order constructs were modeled as formative because they are defined by their lower-order constructs (see Fig. 2), with each lower-order construct constituting one of its facets (Lee & Cadogan, 2013; Petter, Straub, & Rai, 2007). In addition, the higher-order constructs must be modeled as formative in this case because: (a) the lower-order constructs cannot covary since the themes that they represent are distinctive (Petter et al., 2007); and (b) the lower-order constructs are not conceptually identical[5] . For each of the three higher-order constructs, the corresponding lower-order constructs are presented in the following subsections.

4.2.1. Primary appraisal: measurement of BYOD-related threat

BYOD-related threat is measured using two lower-order reflective constructs, *perceived severity* and *perceived vulnerability*, borrowed from the threat appraisal constructs of another coping-based framework: the protection motivation theory (PMT) (Rogers, 1983). The PMT has been adapted to the ISS context (Aurigemma & Mattson, 2019; Lee & Larsen, 2009; Siponen, Mahmood, & Pahnila, 2014; Vance et al., 2012) and more specifically to smartphone protection (Tu et al., 2015) and smartphone-related threats (Weeger et al., 2016; Whitten, Hightower, & Sayeed, 2014).

In line with the PMT and in the context of BYOD usage, we assessed the managers' *personal* perceptions of vulnerability and severity to security breaches, affecting *organizational* data.

- *Perceived vulnerability* is the probability that an unwanted ISS incident (such as loss of data availability, data loss, etc.) occurs (Vance et al., 2012) if no coping behavior is undertaken.
- *Perceived severity is* the level of the potential impact of the threat (Vance et al., 2012) resulting from insufficient or ineffective ISS measures to manage the threat. This perception of potential impacts is important when considering suitable corrective actions to implement (Mustafa et al., 2020) and reinforce the threat appraisal (Siponen et al., 2014).

In our model, *BYOD-related* threat appraisal corresponds to a higher-order construct composed of *Perceived vulnerability* and *Perceived severity* (see Fig. 2).

4.2.2. Primary appraisal: measurement of BYOD-related opportunity

We assessed the managers' perceived benefits related to BYOD usage by employees as a composite formed by *Business process improvement* (Law & Ngai, 2007), *Cost advantages* (Benlian & Hess, 2011) and *Performance expectancy* (Moore & Benbasat, 1991; Venkatesh et al., 2003).

- *Business process improvement* corresponds to the simplification and improvement of business practices and processes through re-engineering (Law & Ngai, 2007), resulting in tangible benefits related to BYOD usage by employees (Leclercq-Vandelannoitte, 2015a; Steelman et al., 2016). Kim, Jang, and Yang (2017) showed that this construct had a strong and significant effect on perceived opportunity.
- *Cost advantages:* Many managers seek to take advantage of the potential benefits of BYOD usage, such as cost savings (Steelman et al., 2016). Permitting the use of BYOD allows companies to avoid buying mobile devices. In addition, companies can also save money when free or low-cost mobile consumer apps are integrated into the corporate infrastructure by employees or when employees store corporate data externally, in the cloud, for example (Weiss & Leimeister, 2012). Benlian and Hess (2011) highlighted cost advantages as the strongest driver influencing managers' perceptions of opportunities.
- *Performance expectancy* is "*the degree to which using an innovation is perceived as being better than using its precursor*" (Moore & Benbasat, 1991, p. 196). Another perceived opportunity is the increase of productivity and innovation stemming from BYOD, resulting in better performance (Tu & Yuan, 2015).

Opportunity appraisal was modeled as a higher-order construct composed of these three dimensions (see Fig. 2).

4.2.3. Secondary appraisal: measurement of perceived behavioral control

The CMUA postulates that the coping strategies depend on the perception of the event (opportunity and/or threat) and on the perceived behavioral control (high or low) over the individual's resulting coping behavior (Beaudry & Pinsonneault, 2005). Perceived behavioral control was modeled as a higher-order variable composed of two dimensions (see Fig. 2):

- *Control over BYOD regulations measures implementation:* when the primary appraisal is associated with an opportunity, this perceived control relates to the implementation of processes and regulations in order to maximize the benefits of BYOD usage;
- *Control over BYOD-related security measures implementation*: when the primary appraisal is associated with a threat, this perceived control

[4] For the rest of this work, we use the terms "higher-order" and "lower-order" constructs as equivalent to "second-order" and "first-order" constructs, respectively.

[5] Lee and Cadogan (2013) demonstrated that higher-order reflective models are not valid when the first-order constructs are not conceptually identical.

relates to the implementation of protective measures in order to reduce either the tensions or the risks emanating from BYOD usage.

4.3. Questionnaire and scales

The questionnaire and the scales used in this research (see Appendix A) were adapted from previous studies:

- The *business process improvement* (BPI) items were adapted from Law and Ngai (2007), the *cost advantages* (CA) scales came from Benlian and Hess (2011), and *performance expectancy* (PERF) was borrowed from Moore and Benbasat (1991);
- The *perceived severity* (SEV) and *perceived vulnerability* (VULN) scales were adapted from Vance et al. (2012) and Siponen et al. (2014);
- The *perceived control over BYOD regulation measures implementation* and *over BYOD-related security measures implementation* scales were adapted from Elie-Dit-Cosaque and Straub (2011) and Vance et al. (2012), respectively; and
- The items used to assess the four coping strategies were adapted from Beaudry and Pinsonneault (2005); Elie-Dit-Cosaque and Straub (2011) and Workman, Bommer, and Straub (2008).

Most of the Likert-type scales we used originally contained seven-point scales. Following the advice of Goodwin and Goodwin (2016), we aligned all of our construct measurements on seven-point scales anchored at 1 (Strongly disagree) and 7 (Strongly agree). We included in the model three control variables (CVs) (see Fig. 2): *Size* represents the company's size; *Age* represents the respondent's age; and *Education* (EDUC) represents the highest degree achieved by the respondent.

In a classical top-down adoption process, implementation is decided by the company managers. We can assume that managers' opportunity and threat appraisals may differ when BYOD is adopted by employees through a reversed adoption logic. For instance, managers can overestimate the risks before addressing BYOD usage, and their appraisal can also evolve after having experimented with BYOD adoption by employees. Meissonier and Houzé (2010) showed that managers must anticipate the outcomes resulting from the adoption of a technology. Given that individuals' strategies and behaviors can evolve according to the pre- or post-adoption stage (Gupta et al., 2020; Meissonier & Houzé, 2010), we can hypothesize that the managers' coping strategies can also differ before and after addressing BYOD usage in their companies. Through the variable PAST (0 = Before; 1 = After implementation), we assessed whether they had implemented measures addressing BYOD usage.

5. Data analysis and results

To validate the measurements and test the hypotheses, we used partial least squares structural equation modeling (PLS-SEM) analyses. PLS-SEM should be selected when the structural model is complex and includes many constructs, indicators and/or model relationships. In addition, our model includes one or more higher-order constructs and formatively measured constructs (Hair, Risher, Sarstedt, & Ringle, 2019, p. 5). Finally, the PLS-SEM approach has a broad scope and is flexible regarding theory and practice (Hair et al., 2019).

5.1. Descriptive statistics

The average manager's age is 42 years old. In terms of gender, the sample was balanced (51 percent male vs. 49 percent female). The companies included 74.1 % SMEs (32.5 % very small, 22.9 % small, 19.6 % medium enterprises) and 25.9 % large enterprises. Among the 337 valid responses, 159 were before and 178 were after BYOD implementation.

5.2. Model assessment

We adopted a two-stage approach because reflective-formative higher-order constructs (HOCs) and moderator variables were part of the model (Hair et al., 2018, p. 53–54). During the first stage, the scores of the independent and moderator variables were computed. We used the repeated indicators approach to compute the scores of lower-order latent constructs (LOCs), which were added to the data set. The second stage used the LOC scores as indicators of the HOCs and built the interaction terms for the moderator variables. After this two-stage process, we assessed the measurement model; for this purpose, we ran bootstrapping with 5000 iterations to assess the path coefficients' significance and evaluate their values (Hair et al., 2018, 2019).

Indicator Reliability and Constructs' Internal Consistency Reliability (see Table C1 in Appendix C): All of the composite reliability values are greater than 0.7, and all of the AVEs (average variance extracted) exceed 0.5, indicating good convergent validity (Hair et al., 2019). Indicator loadings exhibited satisfactory values (see Appendix B).

Discriminant Validity (see Table C2 in Appendix C): All heterotrait-monotrait ratios of correlations (HTMT) are less than the threshold of 0.85 (Hair et al., 2019; Henseler, Ringle, & Sarstedt, 2015), exhibiting good discriminant validity[6] .

Reflective-formative higher-order construct assessment: The two-stage approach results in weights corresponding to the path coefficients between the LOCs and their corresponding HOCs, i.e., BYOD-related opportunity, BYOD-related threat and perceived behavioral control. For LOCs, all of the tests exhibit satisfactory results (see Appendix D), showing satisfactory internal consistency reliability, convergent validity, and discriminant validity. All of the VIFs (variance inflation factors) are less than 5 (Hair et al., 2018, p. 62); hence, potential collinearity between the LOCs forming the HOCs is not problematic. Finally, all of the paths between LOCs and HOCs are positive, highly significant and relatively balanced (see Table D in Appendix D).

As shown in Table 2, the full model exhibits 11 of 12 significant path coefficients. Meissonier and Houzé (2010) used a "before-after" investigation of IT pre- and post-implementation resistance. Several authors have proved the relevance of distinguishing the two stages to shed light on differences in perception between the two phases (Gupta et al., 2020; Meissonier & Houzé, 2010) and on the changes affecting coping strategies over time (Tobler et al., 2017). Hence, to analyze coping strategies related to BYOD adoption in greater depth, we distinguished between managers having actually implemented measures to address BYOD usage and those having planned this implementation.

5.3. Multigroup analysis: distinguishing between pre- and post-implementation

We conducted a multigroup analysis distinguishing between before and after measures implementation to address BYOD usage. First, to ensure measurement invariance, we applied the MICOM procedure (Henseler, Ringle, & Sarstedt, 2016). We checked configural invariance and then parametric tests with 1000 permutations, which showed that compositional invariance is also established. Therefore, conducting multigroup analysis is meaningful for our study. The sample is balanced as 159 respondents (47 %) had intended to implement and 178 (53 %) had actually implemented measures in their company.

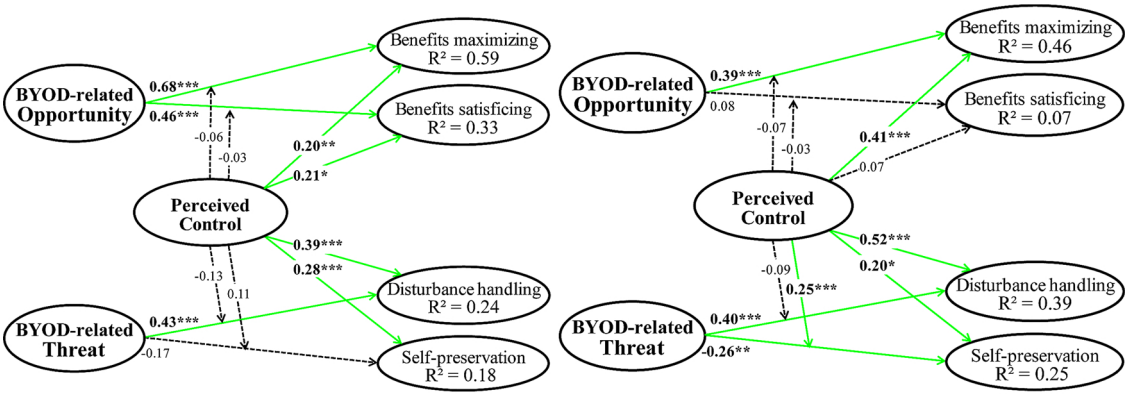
Even if all but one of the path coefficients were significant for the full sample, some of them become nonsignificant for the subgroups, due to smaller populations. Table 2 below illustrates the main discrepancies when comparing before (past = 0) and after (past = 1) implementation. The p-values in the last column indicate whether the differences between path coefficients[7] before and after implementation ('path

[6] Note that, in their 2015 paper, Henseler et al. discarded the Fornell-Larcker and Cross-loadings criteria.

Table 2
Comparison of the constructs' effects for the full sample (n = 337) and before (n = 159) and after (n = 178) implementation of measures.

			Past = 0 (159) Past = 1 (178)							
		Constructs' effects	Path Coeffs (**Full**)	p-values n = 337	Path Coeffs (**past = 0**)	p-values n = 159	Path Coeffs (**past = 1**)	p-values n = 178	Path Coeffs Delta (past 0 vs.1)	p-values of Delta
Opportunity appraisal	Direct effects	H1a: Opportunity - > Benef Maximizing	**0.54**	0.000	**0.68**	0.000	**0.39**	0.000	**0.29**	**0.001**
		H1b: Opportunity - > Benef Satisficing	**0.24**	0.000	**0.46**	0.000	0.08	0.527	**0.38**	**0.008**
		H3a: Perceived Control - > Benef Maximizing	**0.28**	0.000	**0.20**	0.001	**0.41**	0.000	**−0.22**	**0.024**
		H3b: Perceived Control - > Benef Satisficing	**0.18**	0.010	**0.21**	0.015	0.07	0.579	*0.15*	0.165
	Moderating effects	H4a: Perceived Control/ Opport - > Benef Maximizing	**−0.08**	0.026	−0.06	0.402	−0.07	0.118	0.01	0.455
		H4b: Perceived Control/ Opport - > Benef Satisficing	−0.07	0.277	−0.03	0.796	0.03	0.687	−0.05	0.672
Threat appraisal	Direct effects	H2a: Threat - > Disturbance Handling	**0.45**	0.000	**0.43**	0.000	**0.40**	0.000	0.03	0.384
		H2b: Threat - > Self-preservation	**−0.23**	0.000	−0.17	0.068	**−0.26**	0.001	0.09	0.237
		H5a: Perceived Control - > Disturbance Handling	**0.40**	0.000	**0.39**	0.000	**0.52**	0.000	*−0.14*	0.194
		H5b: Perceived Control - > Self-preservation	**0.23**	0.000	**0.28**	0.001	**0.20**	0.043	0.08	0.286
	Moderating effects	H6a: Perceived Control/ Threat - > Disturb Handling	**−0.12**	0.050	−0.13	0.070	−0.09	0.237	−0.04	0.652
		H6b: Perceived Control/ Threat - > Self-preservation	**0.15**	0.007	0.11	0.223	**0.25**	0.000	*−0.14*	0.200

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$.



*** $p<0.001$, ** $p<0.01$, * $p<0.05$

Fig. 3. Path coefficients and significance for Past = 0 (159 managers) and for Past = 1 (178 managers).
*** p < 0.001, ** p < 0.01, * p < 0.05.

coeffs delta') are significant.

Below, we discuss the impact of 'before' and 'after' implementation of measures by managers on the type of coping strategies adopted, first, for the appraisal of BYOD usage as an opportunity, and, second, as a threat. Then, the explanation of R square discrepancies will provide additional insights.

5.3.1. Opportunity appraisal

After organizational measures implementation (past = 1), all but one direct effect decreases, and the moderating effects are not significant regarding the adoption of benefits maximizing and benefits satisficing strategies. The effect of perceived BYOD-related opportunity on the adoption of benefits maximizing strategies decreases (® = 0.68*** ⇨ 0.39***) but remains strong while the effect on benefits satisficing strategies (® = 0.46*** ⇨ 0.08^{NS}) becomes nonsignificant. The influence of perceived control increases (® = 0.20** ⇨ 0.41***) for benefits maximizing strategies and becomes quasi-null for benefits satisficing strategies (® = 0.21* ⇨ 0.07^{NS}). These results reflect that managers' initial expectations of BYOD-related opportunities may be reduced after implementation of measures. The managers' coping strategies aim to increase benefits, capabilities and performance (Fig. 3).

5.3.2. Threat appraisal

Regarding perceived threats, other noticeable while less significant differences appear between the two subgroups. After implementation, the effects of perceived control are much more differentiated for both the disturbance handling and the self-preservation strategies (respectively, ® = 0.52*** and 0.20*) than before implementation (respectively, ® = 0.39*** and 0.28***). The effect of perceived threat remains unchanged after implementation for disturbance handling (® = 0.43*** ⇨ 0.40***), and it becomes significantly negative for self-preservation (® = −0.17^{NS} ⇨ -0.26**). This influence is reinforced by the moderating effect of perceived control on the relationship between threat appraisal and the adoption of a self-preservation strategy. While this effect is not significant before implementation (® = 0.11^{NS}), it becomes much more important (® = 0.25***) after implementation.

This finding may reflect the fact that certain managers stop implementing security measures after a certain time. Interestingly, after retesting the items for the 'after implementation' subgroup, the most influential item is "*potential risks resulting from BYOD cannot affect my company's information security*" (SP2) while "*I gave up taking precautions*" (SP1) becomes less relevant.

Fig. 4 represents the "simple slope analysis" of the moderating effect of perceived control on the relationship between threat appraisal and the adoption of a self-preservation strategy (® = −0.26**). Three lines correspond to moderating effect, at one standard deviation above the mean of the moderator (upper line, +1 SD, +0.25), at the mean of the moderator (central line, null effect, i.e., direct effect of threat only), and at one standard deviation below the mean of the moderator (lower line, −1 SD, −0.25), respectively.

Hence, for high levels of control over the implementation of security measures, managers may believe they are sufficiently protected. This result is illustrated by the upper line in Fig. 4 (slope ~ −0.26 + 0.25 = −0.01).

In contrast, low perceived control over the implementation of security measures strongly and negatively influences managers' self-preservation behavior. The lower line in Fig. 4 exhibits a steeper negative slope (~ −0.26–0.25 = −0.51). Hence, the effect of threat combined with the moderating effect of perceived control (−0.51) compensates for the direct effect of perceived control on self-preservation (® = 0.20*). Consequently, when they perceive low control over the implementation of security measures, managers are discouraged from adopting self-preservation strategies.

All these discrepancies exert cumulative effects on the R square values for the adopted coping strategies (see Table 3).

5.3.3. Analysis of r square discrepancies

The most significant result is the vast decrease in the explanatory power of the model for the benefits satisficing strategy (R^2 = 0.33 ⇨ 0.07) after implementation. This result is explained by the influences of *opportunity appraisal* and *control over implementation* in the adoption of benefits satisficing strategies that were strong before implementation and became nonsignificant after (® = 0.46*** ⇨ 0.08^{NS} and ® = 0.21* ⇨ 0.07^{NS}, respectively).

Referring to the enriched model (see Fig. 2), performance expectancy, cost advantages, and business process improvement become insufficient to satisfy managers. Concretely, maximizing the use of BYOD in their companies becomes their main purpose.

We can assume that after implementation, managers are less engaged in benefits satisficing strategies. The explanatory power of the model before implementation is higher because of high expectations as reflected by the stronger impact of opportunity appraisal.

After implementation, the explanatory power for taking security measures increases (for disturbance handling, R^2 = 0.24 ⇨ 0.39), mainly due to the increase in *perceived control over implementation*. For self-preservation, the explanatory power also increases (R^2 = 0.18 ⇨ 0.25), mainly due to the higher moderating effect of perceived control

[7] For example: for the first line, the path coefficient delta 0.29 corresponds to 0.68–0.39.

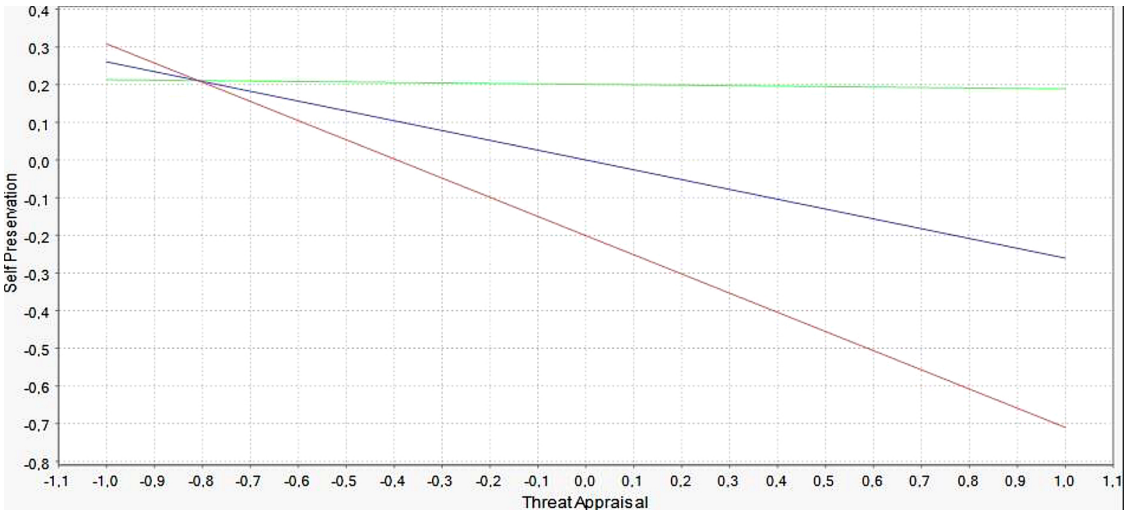


Fig. 4. Interaction plots for high (+1 SD) and low (-1 SD) Perceived Control over security measures implementation.

Table 3
R square discrepancies before and after implementation.

	R square (past = 0)	R square (past = 1)	Delta R^2	p-Value Delta R^2
Benefits Maximizing	0.59	0.46	−0.13	0.061
Benefits Satisficing	0.33	0.07	−0.26	0.005
Disturbance Handling	0.24	0.39	0.15	0.115
Self-preservation	0.18	0.25	0.07	0.388

Table 4
Average value of perceived control constructs before and after implementation.

	Before	After
Perceived control over regulation measures implementation	3.83	5.04
Perceived control over security measures implementation	3.48	4.49

over implementation on the relationship between threat and the self-preservation coping strategy. We can assume that some managers, while having more control over the implementation of security measures, adopt more passive strategies because they think they have reached a satisfactory level of security.

After computing the average value of both *perceived control* variables, it is clear that before implementation, perceived control is below average[8] whereas it increases after implementation (See Table 4).

In our overall model, we noted that while exhibiting strong and significant values, the results for H3b, H5b and H6b were all opposite to what was hypothesized; hence, these hypotheses were not supported. The examination of Tables 2 and 4 allows us to provide another explanation that relativizes our initial hypotheses. We observed that the perception of a threat discourages the adoption of self-preservation strategies (more passive) and encourages the adoption of disturbance handling strategies (i.e., implementing security measures). In contrast, perceived control tends to foster (direct *and* moderating effects) self-preservation strategies. The higher overall influence of perceived control may reflect the fact that, after the implementation of security measures, managers tend to presume a high level of security, as reflected in both retained indicators for the self-preservation strategy: the "*potential risks resulting from BYOD cannot affect my company's information security*" (SP2); therefore, "*I gave up taking precautions*" (SP1).

Consequently, we can assume a "stop-and-start process" restarted by the threat appraisal, which leads to the implementation of information security measures (disturbance handling strategies), results in higher perceived control, and leads to a (false?) sense of immunity, after which no more precautions are implemented (self-preservation strategies). However, the perception of new threats restarts the implementation of new security measures; hence, a cycle is quite possible.

5.4. Common method bias (CMB) assessment

Our results could be subject to common method bias since the survey data were self-reported, and behavior was not actually measured since it resulted from self-assessments by managers (Straub, Limayem, & Karahanna-Evaristo, 1995). Consequently, we adopted the following measures to assess and minimize potential CMB. First, we integrated the a priori procedural remedies recommended by Podsakoff, MacKenzie, and Podsakoff (2012). We used pre-tests to improve our scale items and reduce potential ambiguities, and we broke the routine of questions based on Likert scales by regularly including multiple-choice questions. Second, the path coefficients of the structural model exhibit different levels of significance. Third, we applied Lindell and Whitney's (2001) correlational approach. Hence, we included in our model the blue attitude construct as an a priori "ideal" marker variable (MV) (Simmering, Fuller, Richardson, Ocal, & Atinc, 2015, p. 491), which is theoretically uncorrelated with the other variables included in the model (see Appendix A). The results (see Appendix E) show that the highest correlation between the MV and the latent variables included in our model is 3.46 %, which is far less than the threshold of 9 % (Siemsen, Roth, & Oliveira, 2010). These three elements allow us to believe that CMB is not a critical issue in our study.

6. Discussion

6.1. Implications for theory

The effectiveness of BYOD-related changes depends not only on users' acceptance but also on how managers react to and incorporate employees' initiatives to introduce and use their own devices for business purposes (Leclercq-Vandelannoitte, 2015b). This research builds on this issue and makes several theoretical contributions.

First, our results show that adopted behaviors exhibit significant differences before and after implementation. Before implementing regulating measures, managers can have overrated expectations related to BYOD benefits, and after implementation, these expectations diminish, making way for greater influence of control over implementation, with a positive effect on *benefits maximizing* strategies and negative effects on *benefits satisficing* strategies. Hence, after implementation,

[8] On a Likert 7-point scale, the average value is 4.

perceived opportunity only fosters benefit maximization, and *benefits satisficing* strategies are abandoned. After implementation, the threat appraisal fosters *disturbance handling* and restrains *self-preservation* strategies. A stop-and-start process occurs whereby managers implement security measures, gain perceived control and tend to stop implementing other security measures until new threats are perceived. In addition, the explanatory power of our models is increased after the implementation of coping strategies related to threats, while it decreases for opportunistic coping strategies. These results emphasize the importance of integrating pre- versus post-implementation periods into such studies. Although the previous literature has highlighted the interest of the period (Beaudry & Pinsonneault, 2005; Karahanna et al., 1999; Marler et al., 2009; Taylor & Todd, 1995; Thompson et al., 2006; Veiga et al., 2014; Vieru & Rivard, 2014), it has not investigated the differences between BYOD-related practices before and after IT implementation. Hence, the results of this study make an interesting theoretical contribution to the existing work on MIS linked to specific and ever-growing BYOD practices.

Second, we also extend the current literature on reversed IT adoption and BYOD through the investigation of managers' adaptation strategies to cope with the BYOD phenomenon. Contrary to a classical top-down IT adoption process, BYOD leads managers to react and adapt themselves to a reversed adoption logic over which their control is limited, mainly because they do not own the devices. Their coping strategies reflect how they can address BYOD usage to maximize (or not) the benefits that they perceive —related to BYOD usage by employees— and to minimize (or not) the BYOD-related threats, depending on their own perceptions of the BYOD phenomenon and their perceived control over the regulation measures that they may/should implement.

Third, while the prior research on information security has mainly examined individual compliance and security behaviors, the current study extends this knowledge by investigating the implementation of security measures at an organizational level by managers. On the one hand, this approach provides a more holistic view of BYOD policies which is relatively scarce in the current literature focused on the BYOD usage phenomenon. On the other hand, this approach allows setting the focus on decision-makers in terms of BYOD-related policies and practices.

Fourth, our research extends the previous research on the CMUA. While Beaudry and Pinsonneault (2005) stated that an IT event could be perceived both as an opportunity and as a threat, the qualitative interviews that they conducted with 6 account managers linked each respondent with one coping strategy. Hence, this study has separately investigated opportunities and threats. However, since IT events are multifaceted and encompass both opportunities and threats, they are likely to result in distinctive adaptation strategies (Lazarus & Folkman, 1984). Our work extends the current research because it integrated both types of appraisals by exploring a continuum from threat to opportunity perceptions and permitted us to shed light on the resulting coping strategies. This process also allowed us to identify the differentiated impacts of opportunities and threats on the corresponding strategies. A quantitative study from Elie-Dit-Cosaque and Straub (2011) addressed 168 students: the authors assessed the primary appraisal through scenarios, and the secondary appraisal (level of control) was reduced to a control/no control assessment. Since the authors used scales, they computed the means of their constructs' indicators for each case, instead of conducting more sophisticated analyses, such as structural equation modeling. Our work confirms some of their results: When an IT event is perceived as an opportunity, we can note an important prevalence of *benefits maximizing* over *benefits satisficing* strategies. In the case of a threat, the strategies are much closer, and *disturbance handling* is mainly adopted in the case of high control. However, we do not confirm the link between low behavioral control and the adoption of *self-preservation* strategies. Several explanations can be proposed. First, the population is different (students vs. executives in charge of a team). Executives might react differently than students do. Second, they examined different strategies, with their threat appraisal leading to coping strategies related to lack of interest in new software (*self-preservation*) or failure to achieve better performance with this software (*disturbance handling*), while we focused on strategies to address information security risks (implementing measures for DH and disengagement and denial for SP). Moreover, since their scenarios could distinguish opportunities and threats, the authors could not assess a precise level for the primary appraisal. Using additional constructs for the primary appraisal measurements, we could enrich the CMUA model (see also our last and methodological implication) and obtain a more precise assessment. We contribute to the literature by showing that the primary appraisal exerts a stronger effect on the choice between coping strategies than behavioral control does (secondary appraisal). Bhattacherjee et al. (2018) used the CMUA to investigate individuals' behaviors in the context of mandated IT use. They replaced the usual coping strategies with a typology of behaviors ranging from resistance to acceptance, which reduced the possibilities of comparison with our research. However, they confirmed that emotional and behavioral reactions can coexist and coemerge in response to IT events. Our results underscore that individuals can adopt a spectrum of different types of behaviors (problem and emotion focused) to address specific situations, even in a context of reversed IT adoption. We thus extend the prior research, which mainly considered one type of behavior, such as the intensity of (non-)compliance.

Fifth, we contribute to the literature on emotion-focused (*benefits satisficing* and *self-preservation*) strategies (Liang et al., 2019). These more passive behaviors have been seldom investigated in comparison with more active and problem-focused strategies (i.e., *benefits maximizing* or *disturbance handling* by implementing information security measures) in the context of IT adoption and in the context of ISS. Theoretical contributions on passive behavior are even more important to consider given that a company's employees have an increasingly strong action on the choice of tools they use in a professional context. As a result, the rational proactive actions of managers give greater importance to passive behaviors according to an IT reversed adoption logic (Baillette et al., 2018; Leclercq-Vandelannoitte & Bertin, 2018; Tu & Yuan, 2015).

Finally, from a methodological point of view, this paper fully operationalizes the CMUA through structural equations and extends it through several latent constructs: using formative higher-order constructs, the CMUA was extended to opportunity appraisals with three reflective lower-order constructs borrowed from Kim et al. (2017) and Moore and Benbasat (1991) and to threat appraisals with two reflective lower-order constructs adapted from Rogers' (1983) protection motivation theory (Siponen et al., 2014). In addition, while the prior research has been more qualitative (Beaudry & Pinsonneault, 2005, 2010; Bhattacherjee et al., 2018) or has used calculated average values to distinguish high from low control (Elie-Dit-Cosaque & Straub, 2011), we operationalized the CMUA's "perceived behavioral control" with moderating and direct effects. Significant influences could be identified for the two types of effects with a prevalence of direct influences over moderating effects.

6.2. Implications for practice

Even if the adoption of BYOD is initiated by employees, managers are aware, but only to some extent, of the opportunities and threats associated with BYOD. Our results showed that, when anticipating BYOD adoption by employees, certain managers can expect "just" enjoying the benefits of more performance, limited expenses and improved business processes. However, after having addressed BYOD usage in their company or service, managers are more sensitive to actually maximizing these benefits. Bhattacherjee et al. (2018) showed that the perception of an IT event as an opportunity when feeling great control over the situation was also synonymous with engagement,

which is very important in terms of top management support (Barlette & Jaouen, 2019; Boonstra, 2013). Hence, initially raising managers' awareness and providing guidance regarding concrete means to optimize company performance and enhance business processes with BYOD, while reducing costs, would trigger TMS and thus save time in reaping the benefits from BYOD introduction in their companies.

On the side of BYOD-related threats, addressing the risks is harder. Even if we could identify a stop-and-start process relaunched by the threat appraisal, *self-preservation* behaviors corresponding to denial – "*Risks cannot affect me*"– and distancing – "*I gave up taking precautions*" (see Appendix A) still exist. These behaviors may result not only from higher perceived control over protective behaviors but also from a certain amount of overconfidence, which is common among managers. Managers may not be aware of BYOD-related security issues potentially detrimental to their companies because they are not always actually experienced (Kankanhalli, Teo, Tan, & Wei, 2003). Managers also have difficulties mastering technological innovations that they consider to be the responsibility of IT leaders. For instance, demonstrating through real-life examples the most common security issues and the actual impacts that they had on companies would help to increase managers' perceptions of potential threats (Schuetz, Lowry, Pienta, & Thatcher, 2020). Hence, raising managers' awareness will enhance their *disturbance handling* behaviors, resulting in greater information security for their firms. Managers may also make decisions to improve information security in their company by observing other organizations making the same investment decisions and mimicking their decisions (Shao, Siponen, & Liu, 2020).

Given the importance of achieving a shared understanding of information security policies and measures in companies (Samonas, Dhillon, & Almusharraf, 2020), even if managers are not technically skilled, through higher engagement and top management support (Feng et al., 2019; Indihar Štemberger et al., 2011; Kankanhalli et al., 2003), they could provide more funding and could champion the implementation of security measures, charters, training sessions or awareness-raising campaigns (Herath et al., 2020; Soomro, Shah, & Ahmed, 2016). In addition, TMS would optimize this implementation and favor the adherence of employees (Tobler et al., 2017).

6.3. Implications for policies

This study generates policy implications linked to the recent European regulations on data protection (GDPR[9]). By adding the need to demonstrate compliance with the obligation for security, the GDPR imposes a unified framework for the entire EU with financial penalties. The GDPR strengthens individual rights, empowers individuals' processing of data, and makes the regulations more credible through enhanced cooperation between data protection authorities. The implementation of the GDPR could be an opportunity to review charters and internal policies to clarify, among other things, the processes that should be implemented in the event of theft or loss of a private device or the procedures that should be carried out when an employee leaves a company. These issues are all the more important to be proactively considered in handling new contexts due to emergency situations, such as those encountered in pandemic contexts (Covid-19 for instance), which force organizations to work differently, for instance, favoring remote work and ensuring social distancing. Pandemic contexts can also force employees to use their own mobile devices because, to mitigate the health risks arising from direct contact between people, in lockdown situations, their professional devices are no longer accessible (Davison, 2020; Papagiannidis et al., 2020; Richter, 2020).

Organizations are increasingly supportive of BYOD from a theoretical perspective. However, when it comes to implementing it practically, organizations might hesitate because many personal devices and applications might not comply with such regulations. For example, the threats identified in Section 2.1.2 could lead to increased risks of leaks of personal data –exactly the opposite of what the GDPR aims to achieve. Hence, the practice of BYOD should be increasingly regulated, and the employer should be driven to review its entire organizational policy. Data protection, specifically related to personal data, must be implemented on private devices in accordance with the GDPR. Further, it is the employer, not the employee, who accepts full responsibility. This fact poses major legislative, technical and administrative challenges for both management and IT, particularly when a large number of different devices with specific operating systems and programs must be integrated into the same network. Thus, questioning internal processes and regulating BYOD usage become unavoidable and raise new theoretical issues.

6.4. Limitations and future research

Despite the theoretical, methodological and managerial contributions of this study, several limitations must be considered. First, since the administration of our questionnaire was outsourced, we could not check for or address non-response bias. Second, despite our requirements to include CIOs in our sample, as the respondents were part of a panel, we could obtain only 35 responses. This small number did not permit us to perform significant subgroup analyses such as comparing CIOs with CEOs and other managers. Third, other personality factors and constructs could also play roles in the formation of BYOD-related threatening and beneficial perceptions. Such factors deserve future research. Fourth, the managers' actual BYOD coping strategies were solicited rather than observed. Consequently, self-reported coping strategies might differ to some extent from actual behavior, even if the respondents were guaranteed anonymity.

The explanation proposed for the reversed effect of perceived control on *self-preservation* strategies deserves to be confirmed through further investigation, either through qualitative studies or through more precise questions integrated in future surveys. Using additional constructs borrowed from the 'ways of coping checklist' (Lazarus & Folkman, 1984) would enrich this measurement. In addition, several cognitive biases could influence managers' perceptions and consequently the potential risks or opportunities for firms.

Interest in BYOD-related practices research is increasing due to emergency and disruptive events, such as the current pandemic of Covid-19. Studies of BYOD-related practices will be all the more important to conduct in contexts that require social distancing and remote work performed first out of necessity and then out of habit through the adoption and acceptance of new practices.

More broadly, the results obtained regarding the distinction between pre- and post-implementation could be analyzed over a longer period, owing to a longitudinal study. Future research is needed to further investigate all of these issues.

7. Conclusion

This research applied the CMUA to investigate the adaptation strategies adopted by managers to cope with the BYOD phenomenon. To this end, we analyzed the opportunity and threat appraisals of managers and the impacts on the adopted coping strategies in a context of reversed IT adoption. We extended the CMUA with a set of constructs allowing the assessment of managers' perceived threats and opportunities. Through a survey addressing 337 managers, our article contributes to the academic literature in IS by offering insights into managers' perceptions of BYOD adoption by employees. Four types of coping strategies are investigated and discussed, hereby extending the literature on IT adoption, reversed IT adoption, and information security. An important managerial implication of this paper is the identification of a "stop-and-start" process, reflecting evolution of

[9] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679.

managers' perceptions before and after addressing BYOD usage in their companies. Future research may extend this work, especially to other personality factors and constructs engaged in perceptions of opportunities and threats by managers, as reversed IT adoption is increasingly developing, and managers are known to play a strategic role.

Funding

This research received support from the LabEx Entrepreneurship, University of Montpellier, France, funded by the French government (Labex Entreprendre, ANR-10-Labex-11-01).

CRediT authorship contribution statement

Yves Barlette: Supervision, Conceptualization, Methodology, Investigation, Data curation, Formal analysis, Validation, Resources, Writing - original draft, Writing - review & editing. **Annabelle Jaouen:** Conceptualization, Writing - review & editing, Visualization. **Paméla Baillette:** Conceptualization, Methodology, Investigation, Data curation, Visualization, Investigation, Validation.

Declaration of Competing Interest

The authors report no declarations of interest.

Acknowledgements

Montpellier Business School (MBS) is a founding member of the public research center *Montpellier Research in Management, MRM* (EA 4557, Univ. Montpellier).

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.ijinfomgt.2020.102212.

References

Ali, O., Shrestha, A., Soar, J., & Fosso Wamba, S. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management, 43*, 146–158.

AT&T (2017). *Mind the gap: Cybersecurity's big disconnect – The CEO's guide to cybersecurity*. (Accessed 7 July 2020) https://www.business.att.com/content/dam/attbusiness/reports/cybersecurity-report-v6.pdf.

Aurigemma, S., & Mattson, T. (2019). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems, 20*(12), 1700–1742.

Aydiner, A. S., Tatoglu, E., Bayraktar, E., & Zaim, S. (2019). Information system capabilities and firm performance: Opening the black box through decision-making performance and business-process performance. *International Journal of Information Management, 47*, 168–182.

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs. *Journal of Organizational Change Management, 31*(4), 839–851.

Baillette, P., & Barlette, Y. (2020). Coping strategies and paradoxes related to BYOD information security threats in France. *Journal of Global Information Management, 28*(2), 1–28.

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management, 43*, 76–84.

Baker, J., & Singh, H. (2019). The roots of misalignment: Insights on strategy implementation from a system dynamics perspective. *Journal of Strategic Information Systems, 28*, Article 101576.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management, 52*, Article 102063.

Barlette, Y., & Jaouen, A. (2019). Information security in SMEs: Determinants of CEOs' protective and supportive behaviors. *Systèmes d'Information & Management, 24*(3), 7–40.

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systèmes d'Information & Management, 22*(3), 7–45.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly, 29*(3), 493–524.

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly, 34*(4), 689–710.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT managers. *Decision Support Systems, 52*(1), 232–246.

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management, 8*(3), 1–10.

Bhattacherjee, A., Davis, C. J., Connolly, A. J., & Hikmet, N. (2018). User response to mandatory IT use: A coping theory perspective. *European Journal of Information Systems, 27*(4), 395–414.

Bitglass (2020). *Work from home, securely.* (Accessed 7 July 2020) https://www.bitglass.com/blog/work-from-home-securely.

Boonstra, A. (2013). How do top managers support strategic information system projects and why do they sometimes withhold this support? *International Journal of Project Management, 31*(3), 498–512.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(3), 837–864.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers & Security, 88*. https://doi.org/10.1016/j.cose.2019.101647.

Brodin, M. (2016). BYOD vs. CYOD: What is the difference? *9th IADIS International Conference on Information Systems* (pp. 9–11).

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Chatterjee, S., & Kar, A. K. (2020). Why do small and medium enterprises use social media marketing and what is the impact: Empirical insights from India. *International Journal of Information Management, 53*, Article 102103.

Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: From a citizen's perspective. *Information Technology & People, 32*(5), 1153–1183.

Checkpoint (2020). *Cybersecurity report. Checkpoint research*Tel Aviv. Israel.

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems, 12*(6), 659–673.

Cisco (2016). *3 big risks of BYOD.* (Accessed 7 July 2020) https://www.dmstechnology.com/3-big-risks-of-byod/.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ (USA): Lawrence Erlbaum Associates.

Cook, T., Jaramillo, D., Katz, N., Bodin, W., Cooper, S., Becker, C., et al. (2013). Mobile innovation applications for the BYOD enterprise user. *IBM Journal of Research and Development, 57*(6), 6–10.

Crossler, R. E., & Bélanger, F. (2019). Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research, 30*(3), 995–1006.

Crossler, R. E., Andoh-Baidoo, F. K., & Menard, P. (2019). Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of U.S. and Ghana. *Information & Management, 56*, 754–766.

Crossler, R. E., Bélanger, F., & Ormond, D. (2019). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers, 21*, 343–2357.

D'Arcy, J., & Teh, P. L. (2020). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management, 56*(7), 103–151.

Damanpour, F. (2014). Footnotes to research on management innovation. *Organization Studies, 35*(9), 1265–1285.

Davison, M. (2020). The transformative potential of disruptions: A viewpoint. *International Journal of Information Management*Article 102149.

Ding, J. H., Chien, R., Hung, S. H., Lin, Y. L., Kuo, C. Y., Hsu, C. H., et al. (2014). A framework of cloud-based virtual phones for secure intelligent information management. *International Journal of Information Management, 34*(3), 329–335.

Doargajudhur, M. S., & Dell, P. (2019). Impact of BYOD on organizational commitment: An empirical investigation. *Information Technology & People, 32*(2), 246–268.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. *15th European Conference on Information Systems (ECIS)*.

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51*, Article 102056.

Elie-Dit-Cosaque, C. M., & Straub, D. W. (2011). Opening the black box of system usage: User adaptation to disruptive IT. *European Journal of Information Systems, 20*(5), 589–607.

Fang, X., Benamati, J., & Lederer, A. L. (2011a). Coping with rapid information technology change in different national cultures. *European Journal of Information Systems, 20*(5), 560–573.

Fang, X., Benamati, J., & Lederer, A. L. (2011b). Erratum: Coping with rapid information technology change in different national cultures. *European Journal of Information Systems, 20*(6) 713–713.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*(4), 1149–1160.

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond. *Journal of the Association for Information Systems, 20*(11), 1650–1691.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86*(3), 13–23.
Folkman, S. (1992). Making the case for coping. In B. N. Carpenter (Ed.). *Personal coping: Theory, research, and application* (pp. 31–46). Westport, CT (USA): Praeger Publishers.
Folkman, S., Lazarus, R., Gruen, R., & DeLongis, A. (1986). Appraisal, coping, and health status and psychological symptoms. *Journal of Personality and Social Psychology, 50*(3), 571–579.
Frost, & Sullivan (2016). *Employees say smartphones boost productivity by 34 percent: Frost & Sullivan research.* (Accessed 7 July 2020) https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/.
Garba Bello, A., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information & Computer Security, 25*(4), 475–492.
Gartner (2019). *Open shares in the trenches.* (Accessed 7 July 2020) https://blogs.gartner.com/jay-heiser/2019/01/04/open-shares-in-the-trenches/?_ga=2.233137758.1508062001.1591279319-1972303508.1591279319.
Goodwin, K. A., & Goodwin, C. J. (2016). *Research in psychology: Methods and design* (8th ed.). Hoboken, NJ (USA): John Wiley & Sons.
Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19–28.
Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management, 33*(5), 861–874.
Gupta, A., Yousaf, A., & Mishra, A. (2020). How pre-adoption expectancies shape post-adoption continuance intentions: An extended expectation-confirmation model. *International Journal of Information Management, 52*, Article 102094.
Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM).* Thousand Oaks, CA (USA): Sage Publications.
Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24.
Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2018). *Advanced issues in partial least squares structural equation modeling.* Thousand Oaks, CA (USA): Sage Publications.
Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257–278.
Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Manager, 11*(3), 99–112.
Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135.
Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. *International Marketing Review, 33*(3), 405–431.
Herath, T. C., Herath, H. S. B., & D'Arcy, J. (2020). Organizational adoption of information security solutions: An integrative lens based on innovation adoption and the technology-organization-environment framework. *The Data Base for Advances in Information Systems, 51*(2), 12–35 In Press.
Hoehle, H., Zhang, X., & Venkatesh, V. (2015). An espoused cultural perspective to understand continued intention to use mobile applications: A four-country study of mobile social media application usability. *European Journal of Information Systems, 24*(3), 337–359.
Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35–49.
Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(3), 615–660.
Indihar Štemberger, M., Manfreda, A., & Kovačič, A. (2011). Achieving top management support with business knowledge and role of IT/IS personnel. *International Journal of Information Management, 31*(3), 428–436.
Jarrahi, M. H., Crowston, K., Bondar, K., & Katzy, B. (2017). A pragmatic approach to managing enterprise IT infrastructures in the area of consumerization and individualization of IT. *International Journal of Information Management, 37*(6), 566–575.
Jeong, C. Y., Lee, S. Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management, 56*, 681–695.
Jex, S. M., Bliese, P. D., & Buzzell, S. (2001). The impact of self-efficacy on stressor-strain relations: Coping style as an exploratory mechanism. *Journal of Applied Psychology, 86*, 401–409.
Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management, 35*, 561–571.
Junglas, I., Goel, L., Ives, B., & Harris, J. (2019). Innovation at work: The relative advantage of using consumer IT in the workplace. *Information Systems Journal, 29*, 317–339.
Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139–154.
Karahanna, E., Straub, D., & Chervany, N. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly, 23*(2), 183–213.
Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research, 30*(2), 687–704.
Kaw, J. A., Loan, N. A., Parah, S. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2019). A reversible and secure patient information hiding system for IoT driven e-health. *International Journal of Information Management, 45*, 262–275.
Kemper, G. (2018). *How employees engage with company cybersecurity policies.* (Accessed 7 July 2020) https://clutch.co/it-services/resources/how-employees-engage-company-cybersecurity-policies.
Kim, S. H., Jang, S. Y., & Yang, K. H. (2017). Analysis of the determinants of software-as-a-service adoption in small businesses: Risks, benefits, and organizational and environmental factors. *Journal of Small Business Management, 55*(2), 303–325.
Kim, Y. H., Kim, D. J., & Wachter, K. (2013). A study of mobile user engagement (MoEN): Engagement motivations, perceived value, satisfaction, and continued engagement intention. *Decision Support Systems, 56*, 361–370.
Koch, H., Yan, J. K., & Curry, P. (2019). Consumerization-conflict resolution and changing IT-user relationships. *Information Technology & People, 33*(1), 251–271.
Koch, H., Zhang, S., Giddens, L., Milic, N., Yan, K., & Curry, P. (2014). Consumerization and IT department conflict. *35th International Conference on Information Systems (ICIS)* (pp. 1–15).
Köffer, S., Ortbach, K., Junglas, I., Niehaves, B., & Harris, J. (2015). Innovation through BYOD?: The influence of IT consumerization on individual IT behavior. *Business & Information Systems Engineering, 57*(6), 363–375.
Koohikamali, M., French, A. M., & Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision Support Systems, 119*, 46–59.
Law, C. C. H., & Ngai, E. W. T. (2007). ERP systems adoption: An exploratory study of the organizational factors and impacts of ERP success. *Information & Management, 44*(4), 418–432.
Lazarus, R. S. (1966). *Psychological stress and the coping process.* New York, NY (USA): McGraw-Hill.
Lazarus, R. S. (2000). Toward better research on stress and coping. *American Psychologist, 55*(6), 665–673.
Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping.* New York, NY (USA): Springer Publishing Company.
Leclercq-Vandelannoitte, A. (2015a). Leaving employees to their own devices: New practices in the workplace. *Journal of Business Strategy, 36*(5), 18–24.
Leclercq-Vandelannoitte, A. (2015b). Managing BYOD: How do organizations incorporate user-driven IT innovations? *Information Technology & People, 28*(1), 2–33.
Leclercq-Vandelannoitte, A., & Bertin, E. (2018). From sovereign IT governance to liberal IT governmentality? A Foucauldian analogy. *European Journal of Information Systems, 27*(3), 326–346.
Lee, N., & Cadogan, J. W. (2013). Problems with formative and higher-order reflective variables. *Journal of Business Research, 66*, 242–247.
Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB managers' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187.
Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13–24.
Lian, J.-W., Yen, D. C., & Wang, Y.-T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management, 34*(1), 28–36.
Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(3), 394–413.
Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. (2019). What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. *MIS Quarterly, 43*(2), 373–394.
Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114–121.
Liu, X., & Varshney, U. (2020). Mobile health: A carrot and stick intervention to improve medication adherence. *Decision Support Systems, 128*, 113–165.
Liu, G., Wang, E., & Chua, C. (2015). Leveraging social capital to obtain top management support in complex, cross-functional IT projects. *Journal of the Association for Information Systems, 16*(3), 707–737.
Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546–563.
Marler, J. H., Fisher, S., & Ke, W. (2009). Employee self-service technology acceptance: A comparison of pre-implementation and post-implementation relationships. *Personnel Psychology, 62*(2), 327–358.
McGill, T., & Thompson, N. (2017). Old risks, new challenges: Exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology, 36*(11), 1111–1124.
McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108*, 57–68.
Meissonier, R., & Houzé, E. (2010). Toward an' IT conflict-resistance theory': Action research during IT pre-implementation. *European Journal of Information Systems, 19*(5), 540–561.
Menon, N. M., & Siponen, M. T. (2020). Executives' commitment to information security: Interaction between the preferred subordinate influence approach (PSIA) and proposal characteristics. *The DATABASE for Advances in Information Systems, 51*(2), 36–53.
Middleton, C., Scheepers, R., & Tuunainen, V. K. (2014). When mobile is the norm: Researching mobile information systems and mobility as post-adoption phenomena.

European Journal of Information Systems, 23(5), 503–512.
Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(3), 285–311.
Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192–222.
Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security,* 5–8.
Moser, S., Bruppacher, S. E., & Mosler, H.-J. (2011). How people perceive and will cope with risks from the diffusion of ubiquitous information and communication technologies. *Risk Analysis, 31*(5), 832–846.
Mustafa, S. Z., & Kar, A. K. (2019). Prioritization of multi-dimensional risk for digital services using the generalized analytic network process. *Digital Policy Regulation and Governance, 21*(2), 146–163.
Mustafa, S. Z., Kar, A. K., & Janssen, M. F. W. H. A. (2020). Understanding the impact of digital service failure on users: Integrating Tan's failure and DeLone and McLean's success model. *International Journal of Information Management, 53*, Article 102119.
Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(3), 815–825.
Nokia (2019). *Nokia threat intelligence report 2019*. (Accessed 7 July 2020) https://pages.nokia.com/T003B6-Threat-Intelligence-Report-2019.html.
Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2020). BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2019.1703225.
Papagiannidis, S., Harris, J., & Morton, D. (2020). WHO led the digital transformation of your company? A reflection of IT related challenges during the pandemic. *International Journal of Information Management*Article 102166.
Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*, 409–419.
Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623–656.
Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology, 63*(1), 539–569.
Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(3), 757–778.
Richter, A. (2020). Locked-down digital work. *International Journal of Information Management*Article 102157.
Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo, & R. E. Petty (Eds.). *Social psycho-physiology: A sourcebook* (pp. 153–176). New York, NY (USA): Guilford Press.
Samonas, S., Dhillon, G., & Almusharraf, A. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management, 50*, 144–154.
Schmitz, K. W., Teng, J. T. C., & Webb, K. J. (2016). Capturing the complexity of malleable IT use: Adaptive structuration theory for individuals. *MIS Quarterly, 40*(3), 663–686.
Schuetz, S. W., Lowry, P. B., Pienta, D. A., & Thatcher, J. B. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems* (accepted 14-May-2020).
Shao, X., Siponen, M., & Liu, F. (2020). Shall we follow? Impact of reputation concern on information security managers' investment decisions. *Computers & Security*Article 101961. https://doi.org/10.1016/j.cose.2020.101961.
Siemsen, E., Roth, A., & Oliveira, P. (2010). Common method bias in regression models with linear, quadratic, and interaction effects. *Organizational Research Methods, 13*(3), 456–476.
Simmering, M. J., Fuller, C. M., Richardson, H. A., Ocal, Y., & Atinc, G. M. (2015). Marker variable choice, reporting, and interpretation in the detection of common method variance. *Organizational Research Methods, 18*(3), 473–511.
Singh, N. (2012). B.Y.O.D. Genie is out of the bottle – 'devil or angel'. *Journal of Business Management & Social Sciences Research, 1*(3), 1–12.
Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224.
Sokolova, K., Perez, C., & Lemercier, M. (2017). Android application classification and anomaly detection with graph-based permission patterns. *Decision Support Systems, 93*, 62–76.
Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225.
Srivastava, R., & Tang, T. L.-P. (2015). Coping intelligence: Coping strategies and organizational commitment among boundary spanning employees. *Journal of Business Ethics, 130*(3), 525–542.
Steelman, Z. R., Lacity, M., & Sabherwal, R. (2016). Charting your organization's bring-your-own-device voyage. *MIS Quarterly Manager, 2*(15), 85–104.
Straub, D., Limayem, M., & Karahanna-Evaristo, E. (1995). Measuring system usage: Implications for IS theory testing. *Management Science, 41*(8), 1328–1342.
Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management, 34*(2), 177–184.
Tanenbaum, W. A. (2016). IT systems put security into health care cybersecurity. *Journal of Health Care Compliance, 18*(4), 21–26.
Taylor, S., & Todd, P. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*(2), 144–176.
Thompson, R., Compeau, D., & Higgins, C. (2006). Intentions to use information technologies: An integrative model. *Journal of Organizational and End User Computing, 18*(3), 25–46.
Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*(3), 376–391.
Tobler, N., Colvin, J., & Rawlins, N. W. (2017). Longitudinal analysis and coping model of user adaptation. *Journal of Computer Information Systems, 57*(2), 97–105.
Tu, Z., & Yuan, Y. (2015). Coping with BYOD security threat: From management perspective. *21st Americas Conference on Information Systems (AMCIS)*.
Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management, 52*(4), 506–517.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3–4), 190–198.
Veiga, J., Keupp, M., Floyd, S., & Kellermanns, F. (2014). The longitudinal impact of enterprise system users' pre-adoption expectations and organizational support on post-adoption proficient usage. *European Journal of Information Systems, 23*, 691–707.
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.
Vieru, D., & Rivard, S. (2014). Organizational identity challenges in a post-merger context: A case study of an information system implementation project. *International Journal of Information Management, 34*(3), 381–386.
Wall, J. D., & Warkentin, M. (2020). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management, 56*(8), https://doi.org/10.1016/j.im.2019.03.002.
Weeger, A., Wang, X., & Gewald, H. (2016). It consumerization: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems, 56*(1), 1–10.
Weeger, A., Wang, X., Gewald, H., Raisinghani, M., Sanchez, O., Grant, G., et al. (2020). Determinants of intention to participate in corporate BYOD-programs: The case of digital natives. *Information Systems Frontiers, 22*, 203–219.
Weiss, F., & Leimeister, J. M. (2012). IT innovations from the consumer market as a challenge for corporate IT. *Business & Information Systems Engineering, 4*(6), 363–366.
White, G., Ekin, T., & Visinescu, L. (2017). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems, 57*(4), 353–363.
Whitten, D., Hightower, R., & Sayeed, L. (2014). Mobile device adaptation efforts: The impact of hedonic and utilitarian value. *Journal of Computer Information Systems, 55*(1), 48–58.
Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Dunkan, B. K. (2014). Explaining users' security behaviors with the security belief model. *Journal of Organizational and End User Computing, 26*(3), 23–46.
Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816.
Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44–52.
Xu, F., Lu, X., & Hsu, C. (2020). Anger or fear? Effects of discrete emotions on employee's computer-related deviant behavior. *Information & Management, 57*(3), https://doi.org/10.1016/j.im.2019.103180.
Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*(3), 36–46.
Zhang, L. Z., Mouritsen, M., & Miller, J. R. (2019). Role of perceived value in acceptance of "bring your own device" policy. *Journal of Organizational and End User Computing, 31*(2), 65–82.
Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior, 26*(4), 760–767.
Zhou, Z., Jin, X.-L., Fang, Y., & Vogel, D. (2015). Toward a theory of perceived benefits, affective commitment, and continuance intention in social virtual worlds: Cultural values (indulgence and individualism) matter. *European Journal of Information Systems, 24*(3), 247–261.
Zhou, L., Kang, Y., Zhang, D., & Lai, J. (2016). Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones. *Decision Support Systems, 92*, 14–24.