Coping Strategies and Paradoxes Related to BYOD Information Security Threats in France

Paméla Baillette, Yves Barlette

Journal of Global Information Management
Volume 28 • Issue 2 • April-June 2020

Coping Strategies and Paradoxes Related to BYOD Information Security Threats in France

Paméla Baillette, University of Bordeaux, Bordeaux, France
Yves Barlette, Montpellier Business School, Montpellier, France

ABSTRACT

Bring Your Own Device (BYOD) refers to the provision and use of personal mobile devices by employees for both private and business purposes. Although there has been research on BYOD, little attention has been paid to employees' perception of threats to their personal information security (ISS) when using a BYOD, especially in a professional context. This article investigates employee coping strategies related to BYOD ISS threats in France. The results of a survey of 223 employees indicate that while perceived behavioral control exerts only direct effects on problem-focused (i.e., disturbance handling) and emotion-focused (i.e., self-preservation) coping strategies, ISS concern exhibits significant direct and moderating influences. Several security paradoxes could be identified, namely, discrepancies between the respondents' ISS concern and the adopted coping strategies. This article offers the first insights into the French context and can serve as a basis for comparisons in future research and to help improve employees' personal ISS in the professional context.

KEYWORDS

BYOD, CMUA, Coping, Employees, France, Paradox, Security

INTRODUCTION

Bring Your Own Device (BYOD) refers to the provision and use of personal mobile devices (smartphones, tablets or laptops) by employees for both private and business purposes. This phenomenon reflects a growing "consumerization" trend in information technology (IT), i.e., the adoption in a work context of consumer market technologies (Harris et al., 2012; Jarrahi et al., 2017). An increasing number of companies around the world are being confronted with BYOD, as the worldwide market could represent $318 billion by 2022 (Research and Markets, 2017). Thus, BYOD is of particular interest in that it is said to increase employees' motivation, satisfaction, innovation, levels of comfort, and performance (Harris et al., 2012), offering new productivity gains at the organizational level (Köffer et al., 2015) while reducing technological costs (Singh, 2012). However, this phenomenon also raises technical, security and legal problems (Harris et al., 2012) and entails actual risks for the information security (ISS) of end users' data and devices.

Several studies have investigated security and privacy issues related to mobile device use in a leisure context (Keith et al., 2013, Wottricht et al., 2018). In a professional context, from the organizational point of view, previous research has investigated BYOD adoption and practices by employees (Fujimoto et al., 2016; Lee et al., 2017). The dangers that BYOD poses for organizations have also been investigated (Dang-Pham & Pittayachawan, 2015). However, despite the significant

DOI: 10.4018/JGIM.2020040101

personal ISS concerns expressed by BYOD users (Garba et al., 2017), to the best of the authors' knowledge, no study has addressed employees' protective behaviors related to their own information and tools in the professional context of BYOD, which is the primary and most important knowledge gap addressed by this paper.

In the context of ISS, numerous studies have examined employees' protective behavior (i.e., problem-focused coping strategies), which is separated into two streams: ISS policy compliance (Moody et al., 2018) and the implementation of ISS protective measures (Barlette et al., 2017). Previous studies were focused on the determinants of these problem-focused strategies. However, none explained what happens when an individual does not act and adopts an emotion-focused strategy (i.e., passive) nor provided insight into the determinants of problem-focused (i.e., active) vs. emotion-focused strategies. To fill this second gap, this paper uses the coping model of user adaptation (CMUA). The CMUA has been created to explore behaviors related to the perception of IT events (Beaudry & Pinsonneault, 2005). In the case of threatening IT events, it postulates that individuals can adopt two distinct coping strategies, which are based on the individual's perceived control over this threatening situation. In the case of high control, the adopted coping strategy is problem-focused (i.e., conducting threat-reducing actions); when no behavior alternative is perceived as reliable, the adopted coping strategy is emotion-focused (i.e., denial or passive acceptance) (Beaudry & Pinsonneault, 2005; Moser et al., 2011). Therefore, through the use of the CMUA, adapted to BYOD and ISS contexts, this paper aims to better understand the problem-focused and emotion-focused coping strategies that stem from employees' perceived threats concerning the ISS of their personal data and mobile tools.

However, when addressing the use of mobile phones and applications (Pentina et al., 2016; Wang et al., 2016), numerous privacy-security paradoxes have been noted: Despite substantial information privacy-security concerns, individuals have demonstrated overlooking the ISS of their personal data. Such paradoxes may also occur in the context of BYOD (Harris et al., 2012; Hovav & Putri, 2016). Consequently, ISS concern may also either influence the adopted coping strategy or help reveal ISS paradoxes in the BYOD context; in other words, despite significant security concerns, individuals may remain passive and fail to implement the necessary protective measures. Identifying potential security paradoxes in the adoption of threat-related coping strategies through the CMUA corresponds to the third gap that this paper intends to fill.

In the mobile context, national culture has been shown to influence the perceived ease of use of mobile technologies (Meso et al., 2005; Pentina et al., 2016). With respect to BYOD, French national culture is specific: There are substantial security and privacy concerns related to technical and social constraints, mixed with legal obligations. Moreover, in France, where BYOD is indeed topical, little attention has been devoted to either the perceived threats associated with BYOD adoption and use by employees or the coping strategies stemming from this threat appraisal. This paper also aims to provide insights into the French context to serve as a basis for comparisons in future research.

Given the above considerations, the aims of this paper are (1) to address employees' protective behaviors related to their personal information and devices in the professional context of BYOD, (2) to offer a better understanding of the problem-focused and emotion-focused coping strategies stemming from employees' perceived threats through the use of the CMUA, (3) to identify potential security paradoxes in the adoption of these coping strategies and (4) to realize these aims in a French context.

The main theoretical contributions of this paper are its adaptation of the CMUA to the ISS context and the identification of significant effects of perceived behavioral control and ISS concern. While perceived behavioral control exerts only direct effects on problem-focused and emotion-focused coping strategies, ISS concern exhibits significant direct and moderating influences. Several security paradoxes could be identified, i.e., discrepancies between the respondents' ISS concern and the adopted coping strategies. This paper's main managerial contributions are as follows. First, this article highlights the importance of developing employees' perceived behavioral control to foster the adoption of more active security behaviors and to reduce passivity, given the importance of personal

information and devices to employees. Second, this article provides an overview of the French context and highlights its specificities both in Europe and abroad.

The paper is structured as follows. Section 2 reviews previous research. Section 3 introduces the model and hypotheses. Section 4 presents the adopted methodology. Section 5 gives the results. After discussing the results, Section 6 highlights this paper's theoretical and managerial contributions and suggests avenues for future research.

LITERATURE REVIEW

BYOD and Information Security

Several studies have investigated the adoption and use of personal mobile devices and applications in a leisure or private context (Shin & Choo, 2012; Wakefield & Whitten, 2006), mainly addressing security and privacy issues when using social networks, mobile commerce, sensitive apps (Chatterjee et al., 2017; Pentina et al., 2016; Wottricht et al., 2018) or website customization/personalization (Khatwani & Srivastava, 2017; Keith et al., 2013; Sheng et al., 2008). Other studies have addressed the risks of losing personal data or the loss or theft of one's personal device (Tu et al., 2015). In a professional context, from the organizational point of view, previous research has investigated BYOD adoption by employees (Lee et al., 2017; Weeger et al., 2016) and its impact on new organizational practices (Leclercq Vandelannoitte, 2015). Employees' BYOD-related behavior has been examined in terms of work overload and blurring the frontiers between an employee's private and professional life (Fujimoto et al., 2016; Yun et al., 2012). Studies addressing the impact of BYOD tools and related practices have shown that employees are not aware of their companies' BYOD-specific ISS policies (Crossler et al., 2014) and can be reluctant to comply with these policies when using their own devices (Hovav & Putri, 2016). The dangers that BYOD poses to organizations has also been investigated (Dang-Pham & Pittayachawan, 2015; Harris et al., 2012). However, BYOD users have expressed significant concerns about their own information and devices (Garba et al., 2017) because adopting BYOD also results in greater personal risks.

Numerous theories have been adapted to the IT and ISS contexts to examine the protective behavior of employees. Two distinct streams have investigated compliance with (Moody et al., 2018; Siponen et al., 2014; Vance et al., 2012) or implementation of (Barlette et al., 2017; Boss et al., 2015; Lee & Larsen, 2009) ISS measures and policies. For that purpose, several models or frameworks were used, including the health belief model (Ng et al., 2009), the technology threat avoidance theory (Liang & Xue, 2009), the deterrence theory (Straub, 1990), and Rogers' (1983) protection motivation theory (PMT), that have become very popular in ISS (Lee & Larsen, 2009; Moody et al., 2018). More specifically, several studies adapted these theories to the effect of smartphone-related threats (1) on BYOD adoption (Weeger et al., 2016; Whitten et al., 2014), (2) on compliance with smartphone security policies from the organizational point of view (Crossler et al., 2014), and (3) on smartphone protection in a leisure context (Tu et al., 2015). Other studies have focused more specifically on the case of smartphone-related privacy (Kehr et al., 2015; Sutanto et al., 2013), still in a leisure context.

Previous research investigated the determinants of engaging (or not engaging) in protective behaviors (problem-focused strategies). However, none of the previous studies using coping-based models explain what happens when an individual does not exert protective behaviors (emotion-focused strategies) or compare emotion-focused with problem-focused strategies in a unique model (see Appendix F). Consequently, it has become necessary to formulate another framework.

The Coping Model of User Adaptation

The CMUA was created by Beaudry and Pinsonneault (2005) based on Lazarus' (1966) coping theory. Beaudry and Pinsonneault (2005) adapted the coping theory to IT events. Further studies have since confirmed the insights offered by the CMUA (Beaudry & Pinsonneault, 2010; Elie-Dit-Cosaque &

Straub, 2011). Coping is defined as "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). When confronted with events such as opportunities or threats, individuals perform adaptive behaviors and use two key sub-processes. The primary appraisal consists of evaluating the potential consequences of an event and the personal significance of that event (Folkman, 1992). The secondary appraisal refers to the evaluation of the coping options available. Individuals can adopt two kinds of coping strategies or coping efforts, categorized as problem-focused or emotion-focused, depending on the degree of control they exert over the situation and the potential coping strategy they can adopt. In the case of high perceived control over a threatening IT situation (Beaudry & Pinsonneault, 2005, 2010; Elie-Dit-Cosaque & Straub, 2011), the adopted coping strategy is problem-focused (i.e., it involves threat-reducing actions), and when no behavior alternative is perceived as reliable, the strategy is emotion-focused. Hence, the CMUA provides insights into employees' threat-reducing actions and when they do not act, it also provides insights into emotion-focused strategies such as denial, passive acceptance or the minimization of consequences (Beaudry & Pinsonneault, 2005; Moser et al., 2011).

Primary Appraisal of a Threat

The implementation of BYOD-related practices increases the convergence between private and digital lives. Prior research has found that employees fear that participating in a BYOD program will potentially compromise their private lives and harm the personal data they have stored on their device (Weeger et al., 2016). The risk of mobile loss (or theft) and unauthorized access to personal information stored onto the device is also considered a threat (Tu et al., 2015). Thus, the main danger of BYOD for employees is reflected by their personal information security, which corresponds to the preservation of the confidentiality, integrity and availability of their personal information and devices.

The confidentiality of personal information partially reflects individuals' desire to preserve their information privacy, e.g., to avoid disclosure of their personal information to undesired third parties without their consent (Hong & Thong, 2013; Treiblmayer & Chong, 2011). Integrity problems include cases in which certain types of personal information are damaged or even erased from a personal device. Availability issues correspond to situations in which individuals cannot access their own information or device (theft or loss), a problem that can cause significant setbacks in their daily lives (Jones & Chin, 2015). This concept of personal ISS has been widely highlighted in the literature since the 2000s (Fogel & Nehmad, 2009; Hoadley et al., 2010) and is becoming increasingly important (Kukard & Wood, 2017).

Because the CMUA is based on the original coping theory (see Appendix F), it suffers from a weakness when assessing the primary appraisal of a threat. Indeed, the coping theory is "mute regarding what elements of a disruption are used in primary appraisal" (Beaudry & Pinsonneault, 2005, p.498). Consequently, two constructs were borrowed from another coping-based theory, i.e., the PMT (Rogers, 1983). Thus, the threats related to using personal devices for business purposes are assessed through the individual's perceived vulnerability (e.g., the probability) of the potential event and the individual's perceived severity (e.g., the impact) of the event when it materializes. Perceived vulnerability is the conditional probability that a threatening event will occur, provided either that no adaptive behavior is performed or that there is no adaptation of an existing behavior (Lee & Larsen, 2009). Several studies support the effect of perceived vulnerability in the threat appraisal process and its relationship with the behavioral intention to protect one's self (Lee & Larsen, 2009; Liang & Xue, 2009; Siponen et al., 2014). Perceived severity corresponds to the perception of the severity of the consequences of an ISS problem because previous ISS measures have been either insufficient or ineffective (Liang & Xue, 2009). Perceived severity increases the perception of an event as a threat (Johnston, Warkentin, & Siponen, 2015; Siponen et al., 2014; Vance et al., 2012). In the model in Figure 1, these two constructs represent the underlying formative dimensions of the threat appraisal construct. This primary appraisal entails a secondary appraisal, depending on the

perceived control over the situation and potential coping behaviors (Beaudry & Pinsonneault, 2005; Lazarus & Folkman, 1984).

Secondary Appraisal: Perceived Behavioral Control and Coping Strategies

Coping-based theories postulate that individuals' perceived control over a situation shapes their perceptions of disruptive IT events and influences their subsequent strategy of adaptation (Lazarus & Folkman, 1984; Beaudry & Pinsonneault, 2005). Thus, in case of a threatening event (see Appendix F), high levels of perceived control are associated with threat-reducing actions (problem-focused, i.e., disturbance handling), while for low levels of perceived control, when no behavior alternative is perceived as reliable, people adopt emotion-focused strategies (i.e., self-preservation).

Perceived control over an IT event and an adaptation strategy has been adapted to the context of threatening ISS events in the PMT (Lee & Larsen, 2009; Siponen et al., 2014; Vance et al., 2012). PMT uses self-efficacy that corresponds to the degree of mastery individuals have over IT features and functionalities (e.g., taking protective measures such as implementing an antivirus, performing backups, etc.). Vance et al. (2012, p. 190) define this perceived control as "the degree that the individual believes it is possible to implement the protective behavior." In this study, the underlying protective behavior has been adapted to the context of BYOD and corresponds to implementing data protection measures on the user's personal device. Therefore, a high level of perceived control over device protection will lead individuals to prevent the occurrence of the negative event, i.e., they will implement protective measures. In contrast, when individuals feel they have limited control over the threatening event, they will opt for an emotion-focused coping strategy, i.e., a more passive coping strategy (Beaudry & Pinsonneault, 2005). Workman et al. (2008) investigated the omission of ISS measures: Individuals may be well aware of ISS threats and have knowledge about preventative countermeasures, but if they believe that they do not have the ability to take protective measures to prevent a threat, they are more likely to omit these security measures. Thus, when no behavior alternative is perceived as reliable, people may adopt nonprotective responses (Moser et al., 2011), and the stress resulting from the threat is reduced by adopting several types of adaptation efforts, such as the minimization of consequences, passive acceptance, denial, selective attention, positive comparison and distancing (Beaudry & Pinsonneault, 2005; Moser et al., 2011).

The French Context

In the mobile context, national culture plays an important role in the ease of use of mobile technology (Meso et al., 2005; Pentina et al., 2016). In France, national culture is specific: There are significant security and privacy concerns related to technical and social constraints mixed with legal obligations. On a technical level, application deployment linked to legal obligations constitutes an obstacle for many French firms that generates lags in the use of personal devices. It is difficult and often takes a long time for those firms to deploy, secure and maintain professional applications on heterogeneous mobile devices while respecting employee privacy. On a social level, French companies must negotiate the issue of work-life balance with social partners, and BYOD is one of the ways to break the link between these two spheres. It should also be noted that France remains affected by the phenomenon of work stress (France Telecom, La Poste, Renault in particular).

These constraints are all the stronger because they are mixed with legal obligations, and legislators are increasingly vigilant. The "Right to disconnect,"[1] which entered into force in France in early 2017, is aimed at ensuring the preservation of employees' family and personal lives. With respect to the protection of employees' personal data, the French "Data Protection Authority" (DPA) notes that employers must ensure company data security, even if those data are stored on terminals over which employers have no physical or legal control but have authorized to access and use their professional resources. With respect to the French "Right to be Forgotten" (RTBF), which affects both personal and professional data, France is also different: French people are the source of 20.4% of URL deletion requests linked to their names, even though France represents only 9% of the European population

(Google, 2018). Germans and English people are also very concerned about this issue: France, Germany, and the United Kingdom together generated 51% of URL delisting requests (Google, 2018). By comparison, in the U.S., "legal forgiveness is not offered lightly" (Jones, 2016, p. 141), because legal experts assert that such a law would violate the Constitution's free-speech protections (Glazer, 2015).

Data protection has been stronger in France since the EU's April 2016 adoption of a new legal framework, the "General Data Protection Regulation" (GDPR),[2] which was intended to ensure the protection of European users' privacy and was made directly applicable to the countries of the EU in May 2018. The GDPR also imposes European data protection rules on all foreign firms that handle European consumers' digital information.[3] This development is new and important, as different countries currently take different approaches to data protection: For example, in the U.S., privacy is considered a property right and can be traded on the market. Note that most countries outside Europe have both a strong digital culture and much more flexible legislation, which together favor the development of BYOD, especially in the U.S. (Steelman et al., 2016; Lee et al., 2017), Australia (Imgraben et al., 2014; Garba et al., 2017), and Indonesia (Hovav & Putri, 2016), with a slight advance (Bradley et al., 2012) in the use of BYOD by the U.S. and India. In contrast, Internet access remains highly regulated in Mexico and China. However, BYOD-related practices are increasingly developing in most countries, a development that is particularly attributable to firms' integration of Millennials, Digital Natives and Generation Z, all of whom are asking for communication and flexibility and more broadly, a better balance between their personal and professional lives (Dang-Pham & Pittayachawan, 2015; Nielsen, 2016, 2017). Many international companies, including Apple, Citrix Systems, Unisys, Cisco, the White House, Colgate-Palmolive, and Ford Motor Company, act in favor of BYOD. In this context of strong interest in personal mobile tools, security paradoxes may occur.

From Information Security Concern to Security Paradoxes

Although several studies have addressed privacy concerns in the case of leisure-oriented smartphone use (Pentina et al., 2016; Sutanto et al., 2013), prior research has found that in a BYOD context, employees are also concerned about the risk of mobile loss (or theft) and the risk to the personal information stored on their devices (Tu et al., 2015; Weeger et al., 2016). Therefore, in this paper, information security concern is derived from "privacy concern," which is defined as "an individual's general tendency to worry about information privacy" (Li et al., 2011, p.5). ISS concern may enable the identification of security paradoxes by juxtaposing individuals' expressed ISS concern with their primary appraisal (threatening) and the appropriateness of their adopted coping strategy. Pentina et al. (2016) have examined the direct effect of personal information concern on both the intention to use and the actual use of information-sensitive mobile apps. When "security paradoxes" occur, specific factors may override other factors and lead individuals to endanger their data despite their general concerns (Baillette et al., 2018; Keith et al., 2013; Li et al., 2011). ISS concern is therefore important when assessing such situations: Security paradoxes may occur when there is a discrepancy between the adopted coping strategy and the individual's ISS concern.

HYPOTHESES DEVELOPMENT AND CONCEPTUAL MODEL

Primary Appraisal and Perceived Threat

Previous research has shown that the perception of an event as a threat (Siponen et al., 2014; Vance et al., 2012) leads individuals to behave more cautiously (Bulgurcu et al., 2010). In the context of mobile devices, previous studies have also found that higher perceived threats are positively associated with the adoption of problem-focused (disturbance handling) strategies, i.e., the intention to implement countermeasures (Tu et al., 2015). Conversely, higher perceived threats negatively influence the adoption of emotion-focused (self-preservation) coping strategies (Workman et al., 2008). Therefore, we propose the following hypotheses:

- H1a-b: The perception of a higher BYOD-related threat will (a) positively influence the adoption of a disturbance handling strategy and (b) negatively influence the adoption of a self-preservation strategy.

Secondary Appraisal: Impact of Perceived Control

When a situation is perceived as threatening, the available coping strategies create two alternatives (Beaudry & Pinsonneault, 2005; Moser et al., 2011): High levels of perceived control over information protection are associated with threat-reducing actions (problem-focused coping), while when no behavior alternative is perceived as reliable, people choose nonprotective responses (emotion-focused coping).

The CMUA also postulates that the individual's belief in his/her ability to adapt to a specific situation moderates the relationship between appraisal and coping (Beaudry & Pinsonneault, 2005, p. 520), i.e., it exerts moderating effects on the relationship between the perceived threat and the problem-focused (disturbance handling) and emotion-focused (self-preservation) strategies.

However, prior research in ISS has found that in the case of threatening events, increased coping efficacy also exerted direct effects. Higher levels of coping efficacy exerted direct and positive effects on the adoption of protective responses (Lee et al., 2009, Vance et al., 2012) and direct and negative effects on the adoption of nonprotective, i.e., emotion-focused responses (Moser et al., 2011; Workman et al., 2008).

Consequently, to identify the type of effect, H2 was added to address a potential direct effect, while H4 was added to address a potential moderating effect that is similar in strength and direction (Figure 1). Therefore, the following hypotheses are proposed:

- H2a-b (direct effect): When individuals appraise a situation as a threat, the more perceived control they have over their personal device protection, (a) the more inclined they will be to adopt a disturbance handling strategy, and (b) the less inclined they will be to adopt a self-preservation strategy.
- H4a-b (moderating effect): When individuals appraise a situation as a threat, the level of perceived control they have over their personal device protection will (a) positively moderate the relationship between a BYOD-related threat and a disturbance handling strategy and (b) negatively moderate the relationship between a BYOD-related threat and a self-preservation strategy.

From Information Security Concern to Security Paradoxes

Prior research has found that personal ISS concern was positively associated with an increase in perceived risk (Hong & Thong, 2013; Kehr et al., 2015; Malhotra et al., 2004). Previous literature has also shown that individuals with stronger privacy concerns were found to adopt more restrictive privacy settings (Utz & Krämer, 2009) and more protective behaviors and privacy policy consumption (Stutzman et al., 2011). Thus, the following hypotheses are proposed:

- H3a-b (direct effect): When individuals appraise a situation as threatening, the higher their personal information security concern, (a) the more inclined they will be to adopt a disturbance handling strategy and (b) the less inclined they will be to adopt a self-preservation strategy.
- H5a-b (moderating effect): When individuals appraise a situation as a threat, the level of their personal information security concern will (a) positively moderate the relationship between a BYOD-related threat and a disturbance handling strategy and (b) negatively moderate the relationship between a BYOD-related threat and a self-preservation strategy.

Contradictory results can lead to the identification of security paradoxes. Thus, a high level of ISS concern with an impact that is opposite from what was hypothesized for H3a-b and H5a-b (for

direct or moderating effects) on the adoption of disturbance handling and self-preservation strategies can reveal security paradoxes. Other paradoxical situations can be revealed if specific subgroups with abnormal behaviors can be identified.

Control Variables

Three control variables were included in the model. First, because men tend to adopt more protective behavior (Lee, 2011), Gender is expected to have an impact on the chosen coping strategy: Being male will be synonymous with adopting more disturbance handling and less self-preservation behaviors. Second, a negative impact of age on protective behaviors was identified (Anderson & Agarwal, 2010; Boss et al., 2015). Consequently, Age is expected to negatively influence disturbance handling behavior and positively influence self-preservation behavior. Third, because the most educated people report greater difficulties in managing privacy controls to ensure their personal ISS (Madden, 2012), Education is expected to negatively influence disturbance handling behavior and positively influence self-preservation behavior.

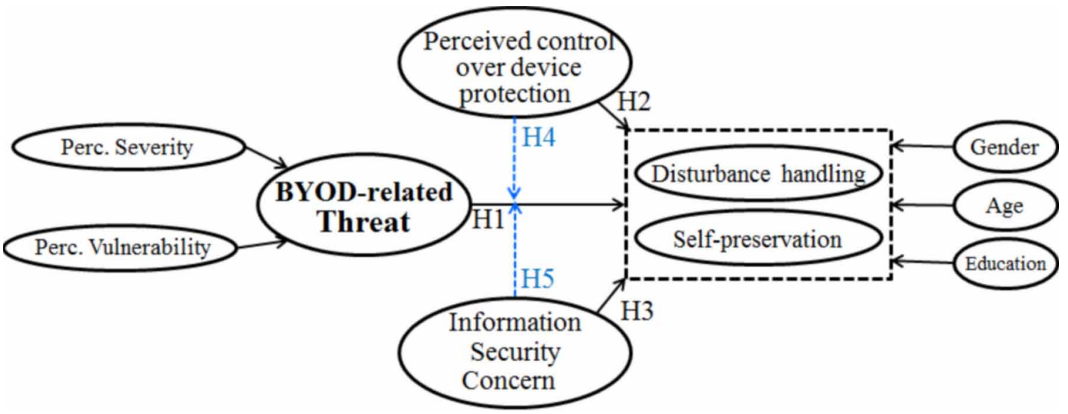
RESEARCH METHOD

Research Design

The survey involved employees currently using or planning to use their own tablet, laptop or smartphone in work settings. The details of the variables and items used in the questionnaire can be found in Appendix A. Those items were first discussed during three professional workshops conducted by the authors on BYOD and then pre-tested through face-to-face interviews with employees (N = 14). Based on the interviewees' feedback, the questions' readability and understandability were improved through several rounds. The web-based questionnaire was created using the Qualtrics tool. At the beginning of the questionnaire, an introductory section presented the purpose of the study and defined the major terms (BYOD, personal device, information security, etc.). Participation in the study was voluntary, and respondents were assured that individual responses would be treated with anonymity and confidentiality.

A link to this questionnaire was included in an email presenting the survey. The administration of the questionnaire was outsourced by a company to a panel of 12,000 employees during June and July 2017. Three hundred and twelve responses were collected. After removing incomplete and invalid responses, 223 usable responses were obtained. The collected data were analyzed using SmartPLS 3.2.7.

Figure 1. Research model (dotted arrows: moderating effects)



Construct Operationalization

The scales used in this study (see Appendix A) were taken from previously validated research:

- The perceived behavioral control over personal device protection (COSP) scales were adapted from Vance et al. (2012).
- The information security concern (ISC) scales were borrowed from Malhotra et al. (2004).
- The disturbance handling (DH) and self-preservation (SP) strategies scales were adapted from Beaudry and Pinsonneault (2005), Workman et al. (2008) and Moser et al. (2011).

Moderation effects were included using the two-stage approach with standardized values (e.g., for interaction plots in Figure 5). Using standardized values for independent and moderator variables decreases multicollinearity in the structural model introduced by interaction terms (Fassot et al., 2016).

According to Hair et al. (2018), second-order constructs are better predictors of broadly defined behaviors, and they overcome the jangle fallacy. They also enable a reduction in the number of relationships in the structural model, making it more parsimonious and easier to apprehend (Hair et al., 2018, p.40). Hence, "BYOD-related threat" has been operationalized as a second-order reflective-formative construct (Hair et al., 2017b) composed of perceived severity and perceived vulnerability (see Figure 1 and Appendix A).

- The perceived severity (SEV) and perceived vulnerability (VULN) scales used measures adapted from Vance et al. (2012) and Siponen et al. (2014)

All items were measured using 7-point Likert scales anchored at 1 = "Strongly disagree" and 7 = "Strongly agree."

With respect to the control variables, Gender (GEND) was included in the form of a dummy variable (male = 0; female = 1). Age (AGE) represents the respondent's age. Education (EDUC) was measured through a scale anchored from 1 "self-taught" to 6 "MS/MA and higher" (Appendix A).

DATA ANALYSIS AND RESULTS

To validate the measurements and test hypotheses, the authors used a Partial Least Squares Structural Equation Modeling (PLS-SEM) analyses. The PLS-SEM approach has a broad scope and is flexible with regard to theory and practice (Richter et al., 2016); it can also be used to address small sample sizes (Hair et al., 2017b) and second-order constructs (Hair et al., 2017a). Moreover, in large and complex models with latent variables, PLS-SEM is "virtually without competition" (Richter et al., 2016; Wold, 1985).

Descriptive Statistics

In our sample, 54.5% of the respondents were male, and 45.5% were female. The proportion of small and medium-sized enterprises (SMEs) vs. larger companies was approximately 44% vs. 56%. The respondents' average age was 35.1 years.

Model Assessment

Because moderator variables and reflective-formative second-order constructs were part of the model, the two-stage approach was adopted (Hair et al., 2018, pp. 53-54). A first stage, using the repeated indicators approach, computes the first-order latent variable scores (i.e., perceived severity and perceived vulnerability) and adds them to the data set. This first stage also permits to obtain the scores of the independent and moderator variables which are saved for further analysis. The second

stage uses the first-order variable scores as indicators of the second-order variable (i.e., BYOD-related threat) and builds the interaction terms for the moderator variables. The measurement model is then assessed.

Overall Fit

A bootstrapping test was performed on 5,000 iterations (Hair et al., 2017b; Henseler et al., 2016). The model fit was tested through a standardized root mean square residual (SRMR) (Henseler et al., 2016, p. 12). Values of 0.095 for the saturated and estimated models, under the threshold of 0.100, indicate a satisfactory fit (Hair et al., 2017b).

Measurement Model Analysis

Indicator Reliability and Constructs' Internal Consistency Reliability (Appendix B)

All Cronbach's α values exceed 0.7, and all composite reliability values are within the interval [0.7-0.95], indicating that they meet the "satisfactory to good" condition (Hair et al., 2017b). All average variance extracted (AVE) values are over 0.5, indicating good convergent validity of the constructs, as each of which explains more than 50% of the indicators' variance (Henseler et al., 2016).

Discriminant Validity

In Appendix B, the Fornell-Larcker criterion is met because for each construct, the square root of the AVE exceeds the highest correlation with the other constructs (Fornell & Larcker, 1981). All the heterotrait-monotrait ratios of correlations (HTMT) are smaller than 0.85 (Henseler et al., 2015, 2016), showing good discriminant validity.

Second-Order Construct Assessment

The second-order construct BYOD-related threat is modeled as reflective-formative (Tiwana & Konsynski, 2010). The two-stage approach results into weights corresponding to the path coefficients between the first-order constructs and BYOD-related threat (Hair et al., 2018, p. 55). They exhibit high and positive values, highly significant and balanced (0.53 vs. 0.60), which is considered satisfactory. The maximal variance inflation factor (VIF) value for the first-order constructs is 1.506, i.e., considerably below the threshold of 5, and therefore potential collinearity between the variables forming the second-order construct is not a critical issue for this model (Hair et al., 2018, p. 62). More information on the assessment of the validity of the first and second-order constructs can be found in Appendix D.

Structural Model Analysis

The model's predictive accuracy can be assessed using R^2 (Figure 2). R^2 values are close to adjusted R^2 values (less than 4%), thus indicating the satisfactory quality and stability of the results.

The bootstrapping test provides the estimates of standard errors for testing the statistical significance of the path coefficients using Student's t-tests and p values. Figure 3 summarizes the results (see also Appendix C).

Disturbance handling behavior ($R^2 = 0.32$) is mainly triggered by high perceived control over device protection ($\beta = 0.47$***) and ISS concern ($\beta = 0.22$**). Self-preservation behavior ($R^2 = 0.14$) is negatively influenced by perceived control over device protection ($\beta = -0.20$*) and the perception of a threatening event ($\beta = -0.17$*). ISS concern exerts a significant moderating effect on the relationship between BYOD-related threat and disturbance handling ($\beta = 0.11$*).

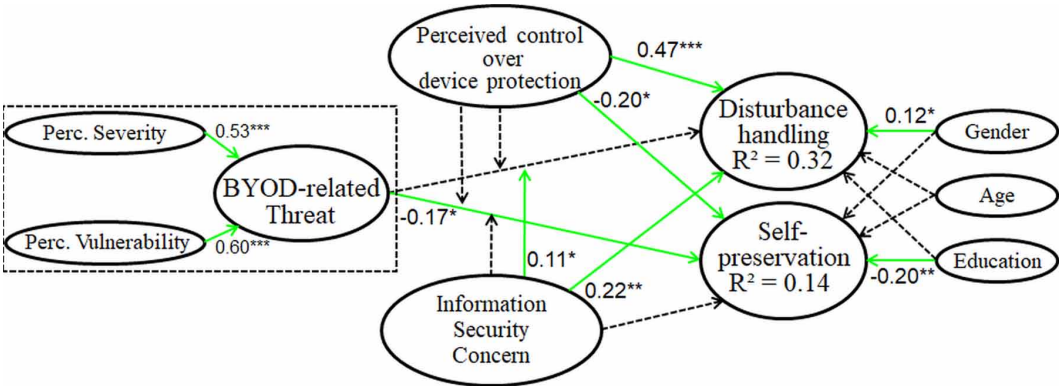
Effects of Control Variables (Appendix C)

Age has no effect on the chosen coping strategies. Men tend to adopt more disturbance handling strategies than women ($\beta = 0.12$*), in line with the expected effect. Education ($\beta = -0.20$**) is a

Figure 2. R^2 for the dependent variables

	R^2	R^2 (adj.)
Disturbance Handling	0.323	0.298
Self-preservation	0.137	0.104

Figure 3. Results and significance of path coefficients[4]; *** p < 0.001, ** p<0.01, * p<0.05



factor that diminishes the adoption of self-preservation (emotion-focused) strategies. This effect is the opposite of what was expected.

Common Method Bias Assessment

Because the survey data were self-reported and can potentially be confounded by common method bias (Podsakoff et al., 2003) and because behavior was self-assessed by respondents and was not actually measured (Straub, Limayem, & Karahanna-Evaristo, 1995), several means of assessing and minimizing the potential common method bias were used.

First, several a priori procedural remedies were used (Podsakoff et al., 2012), including improvements to scale items through pretests to eliminate ambiguities and mixing Likert scales with several yes/no questions or multiple-choice questions.

Second, the marker variable approach was adopted, following the best practices offered by Simmering et al. (2015, p.476). Lindell and Whitney's (2001) correlational technique was used, which has been recently endorsed to provide an indication of the extent to which CMV may be biasing the results of PLS-SEM studies (Malhotra et al., 2015). For that purpose, the research model included an a priori ideal marker variable (MV), the "blue attitude," which is composed of three items (Appendix A) that are theoretically uncorrelated with the variables included in the model. The correlation matrix and detailed results are reported in Appendix E. These results demonstrate that the highest squared correlation between the marker variable and the latent factors included in the model does not exceed 2.37%, a level that is well below the threshold of 9% (Tehseen et al., 2017).

Third, several crosschecks were performed to increase the reliability of the questionnaire. Fourth, the results of the structural model demonstrated different levels of significance for the path coefficients. For all these reasons, CMV bias is unlikely to be a serious concern in this study.

DISCUSSION

Interpretation of Results

Whole Sample Analyses (N = 223)

Effects of Perceived Control

No moderating effect of the respondent's perceived control (Ctrl device protect in Figure 4) could be identified on the relationship between threat appraisal[5] and the adopted coping behavior. Conversely, both direct effects of perceived control on problem-focused and emotion-focused coping behaviors were observed, with a strong positive effect on the adoption of the disturbance handling coping strategy (H2a, $\beta = 0.47$***) and a negative effect on the self-preservation strategy (H2b, $\beta = -0.20$*). This suggests that direct effects should be preferred to moderating effects for threat appraisals, a result that is in line with other ISS-related models (for example, PMT) addressing problem-focused behaviors (Rogers, 1983).

Effects of Threat Appraisal

An event perceived as a threat has no significant effect on the adoption of the disturbance handling strategy (hence H1a is not validated), while it negatively influences self-preservation strategy (H1b, $\beta = -0.17$*).

Effects of Information Security Concern

ISS concern exhibited direct and moderating effects. It exerts a direct and significant effect on the disturbance handling strategy (H3a, $\beta = 0.22$**). It should exert a significant negative effect on self-preservation to discourage the adoption of emotion-focused strategies, although no direct (H3b, $\beta = -0.09^{NS}$) or moderating (H5b, $\beta = 0.09^{NS}$) effect could be identified. Moreover, this last value is positive instead of negative. This absence of effect could indicate a security paradox.

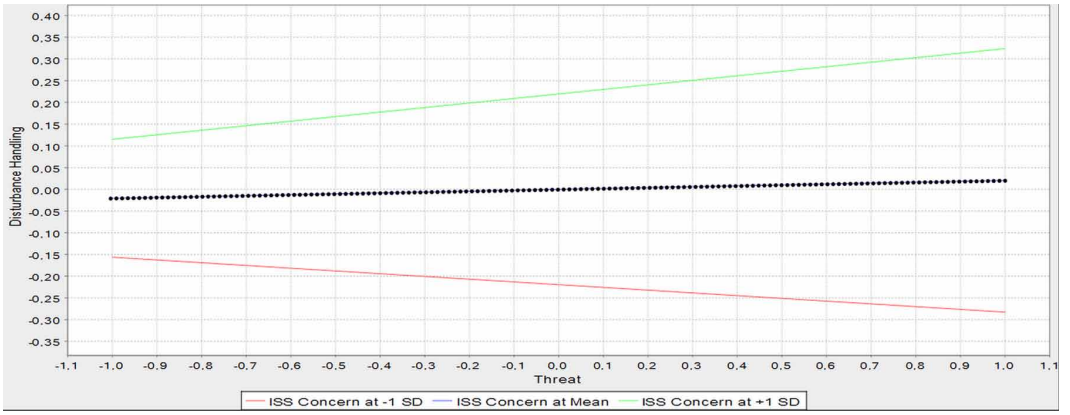
However, ISS concern positively moderates the relationship between the perceived threat and the adoption of a disturbance handling strategy (H5a, $\beta = 0.11$*), meaning that the more concerned the individual, the more protective behaviors in which he or she engages. A slope analysis (Hair et al., 2017b) was conducted to highlight this significant moderating effect of ISS concern (Figure 5).

Figure 4. Variable effects, hypotheses validation and security paradox

# Hyp	Variable influence	Path Coeff.	Student's t-test	P Values	Hypothesis validation	Potential Security paradox
Direct Effects						
1a	Threat -> Disturb Handling	0.021	0.312	0.755	No	
1b	Threat -> Self-Preserv	-0.171	2.308	0.021	Yes	
2a	Ctrl device protect -> Disturb Handling	0.465	7.019	0.000	Yes	
2b	Ctrl device protect -> Self-Preserv	-0.203	2.308	0.021	Yes	
3a	ISS Concern -> Disturb Handling	0.219	3.446	0.001	Yes	No
3b	ISS Concern -> Self-Preserv	-0.091	1.226	0.220	No	NS=> Yes
Moderating Effects						
4a	Ctrl device protect / Threat -> Disturb Handling	-0.038	0.683	0.495	No	
4b	Ctrl device protect/ Threat -> Self-Preserv	-0.030	0.486	0.627	No	
5a	ISS Concern/ Threat -> Disturb Handling	0.113	1.979	0.049	Yes	No
5b	ISS Concern/ Threat -> Self-Preserv	0.060	0.950	0.342	No	NS=> Yes

NS: Non-significant

Figure 5. Interaction plots for high (+1 SD) and low (-1 SD) information security concern



The three lines represent the impact of ISS concern on the relationship between the perceived threat and disturbance handling coping strategy. The dotted line represents the relationship for the mean value of the moderator variable ISS concern. In this case, there is no significant effect. However, the higher line shows that the more the individual is concerned with his/her ISS, the more he/she will adopt disturbance handling behaviors (problem-focused), but the opposite is also true, i.e., for low levels of ISS concern, an individual is less engaged in disturbance handling behaviors (lower line).

Multigroup Analyses

According to Hair et al.'s (2017b) guidelines, the minimum sample size should be greater than 10 times the largest number of structural paths directed at a particular construct in the structural model. As the number of paths directed at any coping strategy is 6, the sample should exceed 60 observations for each analysis. Several multigroup analyses were performed; only the most noticeable analyses, i.e., those revealing significant differences among subgroups, are reported below.

First, the respondent's age was tested considering whether the respondent did (N = 138) or did not (N = 84) belong to the "digital native" generation. This term was coined by Prensky (2001) and corresponds to people born after 1980. Two subgroups were created, distinguishing digital natives from older respondents. The results show that for people born before 1980, ISS concern has a stronger negative impact on self-preservation behaviors (β = -0.30**) than it does for digital natives (β = 0.07^{NS}). People born before 1980 are more likely to protect themselves, as threat appraisal exerts a stronger positive impact on their disturbance handling behaviors (β = 0.36***) than on those of digital natives (β = -0.07^{NS}). For digital natives (37+ years old), ISS concern is never significant, with either direct or moderating effects. The perception of a threatening event has no influence on disturbance handling and self-preservation strategies (Prensky, 2001; Palfrey & Gasser, 2013; Wang et al., 2015). The adoption of a disturbance handling strategy is only influenced by the perceived control of digital natives. These results suggest a security paradox, as threats pertaining to personal information and security concerns should—but do not—have any impact on this population.

Second, firm size was tested, comparing SMEs (N = 122) with larger companies (N = 98). In SMEs, respondents concerned with their ISS are less likely to adopt self-preservation strategies (β = -0.23*) compared with employees who work at larger companies (0.08^{NS}). Other results were very similar to the full sample.

Third, the level of ISS concern was used to distinguish two subgroups (high concern, N = 94, vs. low concern, N = 78[6]). People belonging to the "high security concern" group, who have a high level of control over their device protection, were less likely to adopt a self-preservation coping strategy (β = -0.32***) than employees belonging to the less concerned subgroup ($+0.10^{NS}$).

Note that a subgroup analysis based on education did not provide any significant results.

Highlighting Results in the French Context Compared with Other Countries

In BYOD settings, the results confirm the importance of individuals' perceived behavioral control (Meso et al., 2005; Thompson et al., 2017; Tu et al., 2015) in explaining protective coping behaviors, as previously identified in the USA and Australia. In the French context, perceived behavioral control over device protection exerted the strongest direct effect on the choice of disturbance handling (H2a, $\beta = 0.47$***) strategy. A new insight is that perceived behavioral control also exerts a negative direct effect (the third one in magnitude) on the self-preservation (H2b, $\beta = -0.20$*) coping strategy.

In this study, French people's average ISS concern about BYOD is 5.21 on a 1-7 scale. Pentina et al. (2016) also measured high levels of personal ISS concern in their study of two countries, namely, the USA (5.36) and China (5.61). In both countries, the individual's privacy concern did not appear to play a role in either the adoption of or the intention to use personal information sensitive apps. Their finding was found to support the occurrence of a privacy paradox, as concern did not seemingly affect either intention or actual behaviors with regard to the use of mobile apps that require access to sensitive data, thus endangering their personal data. In the French context, ISS concern was shown to foster disturbance handling strategies (i.e., adopting protective behavior), with both direct (H3a, $\beta = 0.22$**) and moderating (H5a, $\beta = 0.11$*) effects. However, despite high ISS concern, this construct exerted no significant impact, either direct or moderating (H3b and H5b), on self-preservation strategies. However, an increase in ISS concern should negatively influence the adoption of self-preservation strategies (i.e., discouraging passivity). This could also indicate a security paradox.

A personal ISS paradox phenomenon has also been identified in a study performed in a BYOD-enabled Australian university (Dang-Pham & Pittayachawan, 2015). Their study highlights the influence of perceived threats on users' intention to perform protective behaviors. These authors recommend that academics and practitioners raise awareness about the fact that users are not always willing to carefully avoid malware, even when they are engaged in personal activities. In the French context, the perceived BYOD-related threat did not exert any significant impact on the disturbance handling coping strategy (H1a, $\beta = 0.04^{NS}$). Moreover, the subgroup analysis based on the level of ISS concern did not show any impact, even for the higher levels of ISS concern. Therefore, this result could also reveal a security paradox. Conversely, a new insight offered by a model integrating self-preservation strategies is that the negative impact of the perceived threat on passive strategies is stronger for the subgroup with higher ISS concern than for the whole sample ($\beta = -0.32$*** vs. $\beta = -0.17$*, for H1b). This result deserves future research in other countries to provide comparisons.

Theoretical Contributions

This research is the first to address employees' protective behaviors related to their personal information and devices in the professional context of BYOD. For that purpose, the CMUA was adapted to the ISS context, which provided a better understanding of the problem-focused and emotion-focused coping strategies.

This paper is also the first both to model and operationalize the CMUA through structural equation modeling and to extend it via exogenous latent variables to assess individuals' threat appraisal. The CMUA was extended by constructs borrowed from the PMT (Rogers, 1983). The "perceived control over device protection" construct was operationalized with moderating and direct effects. The results show that its effects are only direct, providing insights into how to operationalize this construct in future research. ISS concern was also added to the model with the goal of revealing security paradoxes, as this phenomenon had not been previously addressed in a BYOD context. The results show that ISS concern has direct and moderating effects on the adopted coping strategies. Several security paradoxes could be identified, i.e., discrepancies between employees' personal ISS concern and their choice of problem-focused or emotion-focused strategies. In the field of ISS, this concern deserves more inclusion in models such as PMT or more generally, in all models that investigate coping behaviors.

Finally, this research highlights employees' perceptions of BYOD-related threats in France. ISS concern is an important construct in the French context because employees, especially the younger ones, increasingly rely on their own devices at work and are particularly concerned about preserving their personal information.

Managerial Contributions

This research highlights the importance of perceived behavioral control over device protection: It positively influences disturbance handling strategies (problem-focused), i.e., to engage in protective measures against personal ISS issues or unauthorized access to personal devices in BYOD settings. In companies, a charter therefore could raise employees' awareness of the need for self-training on mobile device protection. Although employees' devices can be very disparate, companies can still provide employees with hints and best practices for protecting their devices, which in turn may increase the company's security.

In the same vein, increasing the perception of potential threats by showing the most common security issues and their potential impacts through real-life examples could decrease self-preservation (emotion-focused) behaviors corresponding to denial ("Risks will not affect me") and distancing ("I cannot do anything") (Appendix A). This reduction in self-preservation behaviors would also result in higher security for employees and their companies.

This study showed that when employees' ISS concern is high, security paradoxes can occur. The impact of security paradoxes corresponds to a reduction in active behavior (problem-focused) in favor of more passive behavior (emotion-focused). ISS concern can be developed through employees' training and awareness raising, which will also reduce the discrepancy between employees' ISS concern and their reported behaviors. Security paradoxes could be decreased through the implementation of more constraining measures, such as charters, BYOD policies, or specific BYOD-related contractual requirements.

Finally, because previous studies have shown that results can vary according to country, training sessions, awareness-raising campaigns and charters could be tailored to various countries' cultures.

Limitations and Avenues for Future Research

Despite the numerous theoretical and managerial contributions of this study, several limitations must be considered. First, respondents' actual BYOD coping strategies were solicited rather than observed: It is possible that actual and self-reported coping strategies differ in practice, even if respondents are guaranteed anonymity. Second, this study was conducted solely in France and, consequently, the results were not compared with those of other countries. Third, other personality factors and constructs also play a role in the formation of threatening perceptions related to BYOD. The addition of other factors to the model would definitely warrant future research. Fourth, at an organizational level, companies that are particularly sensitive to data security issues may implement more restrictive organizational protective measures that increasingly threaten the personal information of BYOD adopters, thus influencing employees' BYOD-related behavior. Fifth, the selection of the respondents was left to the interviewers, as respondents were part of a panel.

Several avenues for future research can be explored. It would be interesting to study the population of digital natives (37+ years old), as significant differences between older individuals could be identified, leading to potential "generational security paradoxes." It would also be useful to compare several generations (Gen X, Y and Z), as studies addressing age differences are still relatively scarce (Lai & Li, 2005). The causes of security paradoxes also deserve exploration, as they may provide valuable insights into how to act on their drivers and barriers to reduce their occurrence. Finally, comparing BYOD-related issues among different countries would provide additional insight, as the importance of country culture was previously observed in the context of mobile applications and stemming behaviors. In the same vein, it would be useful to address the level of concern expressed by employees in different countries about the protection of personal data versus professional data.

CONCLUSION

This paper aimed at better understanding coping strategies stemming from threats perceived by employees concerning the ISS of their personal data in a BYOD context. The research model was built on the threat appraisal part of the CMUA, complemented with the PMT, to provide insights regarding the determinants of problem-focused and active strategies (i.e., disturbance handling) compared with emotion-focused and more passive strategies (i.e., self-preservation). In accordance with the CMUA and previous coping-based studies, perceived behavioral control was modeled as having potential direct and moderating effects. ISS concern proved to be effective on the detection of security paradoxes in leisure contexts, and therefore, this construct was added to the model to identify security paradoxes in the professional setting of BYOD. A survey was conducted among 223 employees in the French context, representing a specific area of study.

This article offers several theoretical and managerial contributions. The main theoretical implication of this paper is this new model, allowing to investigate employees' protective behaviors related to their own information and tools in the professional context of BYOD. The model allows determinants to be identified and problem-focused and emotion-focused strategies to be compared. Second, the results show that perceived behavioral control exerts only direct effects on both coping strategies, while ISS concern exerts both direct and moderating effects, but only on the disturbance handling (problem-focused) strategy. Third, the results highlight security paradoxes, i.e., discrepancies between the respondents' ISS concern and the adopted coping strategies.

This paper's main managerial contributions highlight the importance of perceived behavioral control to the adoption of more problem-focused and active coping behaviors, leading to improvement in employees' personal ISS.

The literature review states that French national culture plays an important role in the adoption of BYOD due to security and privacy concerns related to technical (securing applications on mobile devices) and social (negotiating with social partners) constraints mixed with legal obligations (DPA, RTBF, and GDPR). Therefore, when conducting future research in other countries, it will be important to take into account French specificities before comparing the results. French culture should also be taken into account in the development of training sessions and awareness raising campaigns.

Finally, because this paper identified a very important gap between digital natives and older generations that leads to security paradoxes, the authors suggest conducting future studies in this direction and obtaining comparisons between France and other countries when studying coping strategies in the context of BYOD and personal ISS.

Funding Details

Yves Barlette is member of the Entrepreneurship and Innovation Chair, which is part of LabEx Entrepreneurship (University of Montpellier, France) and funded by the French government (Labex Entreprendre, ANR-10-Labex-11-01).

ACKNOWLEDGMENT

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

REFERENCES

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *Management Information Systems Quarterly*, *34*(3), 613–643. doi:10.2307/25750694

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*(December), 76–84. doi:10.1016/j.ijinfomgt.2018.07.007

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' Information Security Behavior in SMEs: Does ownership matter? *Systèmes d'Information & Management*, *23*(2), 7–45. doi:10.3917/sim.173.0007

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *Management Information Systems Quarterly*, *29*(3), 493–524. doi:10.2307/25148693

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *Management Information Systems Quarterly*, *34*(4), 689–710. doi:10.2307/25750701

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *Management Information Systems Quarterly*, *39*(4), 837–864. doi:10.25300/MISQ/2015/39.4.5

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., & Buckalew, L. (2012). *BYOD: A global perspective. Harnessing employee-led innovation*. Cisco Internet Business Solutions Group. Retrieved from http://resources.idgenterprise.com/original/AST-0074924_BYOD_Horizons-Global.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly*, *34*(3), 523–548. doi:10.2307/25750690

Chatterjee, S., Kar, A. K., & Gupta, M. P. (2017). Critical success factors to establish 5G network in smart cities: Inputs for security and privacy. *Journal of Global Information Management*, *25*(2), 15–37. doi:10.4018/JGIM.2017040102

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226. doi:10.2308/isys-50704

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, *48*, 281–297. doi:10.1016/j.cose.2014.11.002

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. doi:10.1057/ejis.2010.23

Fassott, G., Henseler, J., & Coelho, P. S. (2016). Testing moderating effects in PLS path models with composite variables. *Industrial Management & Data Systems*, *116*(9), 1887–1900. doi:10.1108/IMDS-06-2016-0248

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. doi:10.1016/j.chb.2008.08.006

Folkman, S. (1992). Making the case for coping. In B. N. Carpenter (Ed.), *Personal coping: Theory, research, and application* (pp. 31–46). Westport, CT: Praeger.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *JMR, Journal of Marketing Research*, *18*(1), 39–50. doi:10.1177/002224378101800104

Fujimoto, Y., Ferdous, A. S., Sekiguchi, T., & Sugianto, L.-F. (2016). The effect of mobile technology usage on work engagement and emotional exhaustion in Japan. *Journal of Business Research*, *69*(9), 3315–3323. doi:10.1016/j.jbusres.2016.02.013

Garba, A. B., 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.

Glazer, S. (2015, December 4). *Privacy and the Internet*. CQ Researcher. Retrieved from http://tinyurl.com/h85c83x

Google. (2018). *Three years of the Right to be Forgotten*.

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017a). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, *117*(3), 442–458. doi:10.1108/IMDS-04-2016-0130

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017b). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Thousand Oaks, CA: Sage.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2018). *Advanced issues in partial least squares structural equation modeling*. Thousand Oaks, CA: SAGE Publications.

Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Executive*, *11*(3), 99–112.

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, *116*(1), 2–20. doi:10.1108/IMDS-09-2015-0382

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic Commerce Research and Applications*, *9*(1), 50–60. doi:10.1016/j.elerap.2009.05.001

Hong, W., & Thong, J. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Management Information Systems Quarterly*, *37*(1), 275–298. doi:10.25300/MISQ/2013/37.1.12

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. doi:10.1016/j.pmcj.2016.06.007

Imgraben, J., Engelbrecht, A., & Choo, K.-K. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347–1360. doi:10.1080/0144929X.2014.934286

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. doi:10.1016/j.ijinfomgt.2017.05.016

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Management Information Systems Quarterly*, *39*(1), 113–134. doi:10.25300/MISQ/2015/39.1.06

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*(5), 561–571. doi:10.1016/j.ijinfomgt.2015.06.003

Jones, M. (2016). *Ctrl Z: The right to be forgotten*. New York: New York University Press.

Khatwani, G., & Srivastava, P. R. (2017). An Optimization Model for Mapping Organization and Consumer Preferences for Internet Information Channels. *Journal of Global Information Management*, *25*(2), 88–115. doi:10.4018/JGIM.2017040106

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. doi:10.1111/isj.12062

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. doi:10.1016/j.ijhcs.2013.08.016

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. doi:10.1016/j.dss.2013.07.002

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. doi:10.1007/s12599-015-0387-z

Kukard, W., & Wood, L. (2017). Consumers' perceptions of item-level RFID use in FMCG: A balanced perspective of benefits and risks. *Journal of Global Information Management*, *25*(1), 21–42. doi:10.4018/JGIM.2017010102

Lai, V. S., & Li, H. (2005). Technology acceptance model for internet banking: An invariance analysis. *Information & Management*, *42*(2), 373–386. doi:10.1016/j.im.2004.01.007

Lazarus, R. S. (1966). *Psychological stress and the coping process*. New York: McGraw-Hill.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. New York: Springer Publishing.

Leclercq-Vandelannoitte, A. (2015). Leaving employees to their own devices: New practices in the workplace. *The Journal of Business Strategy*, *36*(5), 18–24. doi:10.1108/JBS-08-2014-0100

Lee, J. Jr, Warkentin, M., Crossler, R. E., & Otondo, R. F. (2017). Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. *Journal of Computer Information Systems*, *57*(4), 309–318. doi:10.1080/08874417.2016.1184032

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*(2), 361–369. doi:10.1016/j.dss.2010.07.009

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. doi:10.1057/ejis.2009.11

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434–445. doi:10.1016/j.dss.2011.01.017

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *Management Information Systems Quarterly*, *33*(1), 71–90. doi:10.2307/20650279

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *The Journal of Applied Psychology*, *86*(1), 114–121. doi:10.1037/0021-9010.86.1.114 PMID:11302223

Madden, M. (2012). Privacy management on social media sites. *Pew Internet Report*.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. doi:10.1287/isre.1040.0032

Malhotra, N. K., Schaller, T. K., & Patil, A. (2017). Common method variance in advertising research: When to be concerned and how to control for it. *Journal of Advertising*, *46*(1), 193–212. doi:10.1080/00913367.2016.1252287

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. doi:10.1080/0144929X.2017.1352028

Meso, P., Musa, P., & Mbarika, V. (2005). Towards a model of consumer use of mobile information and communication technology in LDCs: The case of sub-Saharan Africa. *Information Systems Journal*, *15*(2), 119–146. doi:10.1111/j.1365-2575.2005.00190.x

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *Management Information Systems Quarterly*, *42*(1), 285–311. doi:10.25300/MISQ/2018/13853

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. doi:10.1111/j.1539-6924.2010.01544.x PMID:21175715

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. doi:10.1016/j.dss.2008.11.010

Nielsen. (2016). *Millennials are top smartphones users.* Retrieved from http://www.nielsen.com/us/en/insights/news/2016/millennials-are-top-smartphone-users.html

Nielsen. (2017). *Youth movement: Gen Z boasts the largest, most diverse media users yet*. Retrieved from http://www.nielsen.com/us/en/insights/news/2017/youth-movement-gen-z-boasts-the-largest-most-diverse-media-users-yet.html

Palfrey, J. G., & Gasser, U. (2013). *Born digital: Understanding the first generation of digital natives*. Basic Books.

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. doi:10.1016/j.chb.2016.09.005

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*(5), 879–903. doi:10.1037/0021-9010.88.5.879 PMID:14516251

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. doi:10.1146/annurev-psych-120710-100452 PMID:21838546

Prensky, M. (2001). *Digital natives, digital immigrants*. Retrieved from http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

Research and Markets. (2017). *Global Enterprise Application Market*. Retrieved from https://www.researchandmarkets.com/research/7q48z2/global_enterprise

Richter, N. F., Cepeda, G., Roldán, J. L., & Ringle, C. M. (2016). European management research using partial least squares structural equation modeling. *European Management Journal*, *34*(6), 589–597. doi:10.1016/j.emj.2016.08.001

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 psychophysiology: A sourcebook* (pp. 153–176). New York: Guilford Press.

Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, *9*(6), 344–376. doi:10.17705/1jais.00161

Shin, D.-H., & Choo, H. (2012). Exploring Cross-Cultural Value Structures with Smartphones. *Journal of Global Information Management*, *20*(2), 67–93. doi:10.4018/jgim.2012040104

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: A review and demonstration. *Organizational Research Methods*, *18*(3), 473–511. doi:10.1177/1094428114560023

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. doi:10.1016/j.im.2013.08.006

Straub, D., Limayem, M., & Karahanna-Evaristo, E. (1995). Measuring system usage: Implications for IS theory testing. *Management Science*, *41*(8), 1328–1342. doi:10.1287/mnsc.41.8.1328

Straub, D. W. Jr. (1990). Effective IS Security. *Information Systems Research*, *1*(3), 255–276. doi:10.1287/isre.1.3.255

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, *27*(1), 590–598. doi:10.1016/j.chb.2010.10.017

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *Management Information Systems Quarterly*, *37*(4), 1141–1164. doi:10.25300/MISQ/2013/37.4.07

Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, *4*(2), 142–168. doi:10.20547/jms.2014.1704202

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. doi:10.1016/j.cose.2017.07.003

Tiwana, A., & Konsynski, B. (2010). Complementarities between Organizational IT Architecture and Governance Structure. *Information Systems Research*, *21*(2), 288–304. doi:10.1287/isre.1080.0206

Treiblmaier, H., & Chong, S. (2011). Trust and perceived risk of personal information as antecedents of online information disclosure: Results from three countries. *Journal of Global Information Management*, *19*(4), 76–94. doi:10.4018/jgim.2011100104

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. doi:10.1016/j.im.2015.03.002

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyber psychology: Journal of Psychosocial Research on Cyberspace*, 3(2). Retrieved from https://cyberpsychology.eu/article/view/4223/3265

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. doi:10.1016/j.im.2012.04.002

Wakefield, R. L., & Whitten, D. (2006). Mobile computing: A user study on hedonic/utilitarian mobile device usage. *European Journal of Information Systems*, *15*(3), 292–300. doi:10.1057/palgrave.ejis.3000619

Wang, X., Weeger, A., Gewald, H., Sanchez, O., Raisinghani, M., & Pittayachawan, S. (2015). Determinants of intention to participate in corporate BYOD-programs: The case of digital natives. In *Proceedings of the 75th Annual Meeting of the Academy of Management*, Vancouver, BC Canada, August 7-11.

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. doi:10.1080/08874417.2015.11645795

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. doi:10.1080/08874417.2014.11645740

Wold, H. O. (1985). Partial least squares. In S. Kotz & N. Johnson (Eds.), *Encyclopedia of statistical sciences* (Vol. 6, pp. 581–591). NewYork, NY: Wiley.

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. doi:10.1016/j.chb.2008.04.005

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. doi:10.1016/j.dss.2017.12.003

Yun, H., Kettinger, W. J., & Lee, C. C. (2012). A New Open Door: The Smartphone's Impact on Work-to-Life Conflict, Stress, and Resistance. *International Journal of Electronic Commerce*, *16*(4), 121–151. doi:10.2753/JEC1086-4415160405

ENDNOTES

1 https://www.internationallaborlaw.com/2017/02/02/the-right-to-disconnect-a-new-right-for-french-employees/

2 https://www.cnil.fr/en/press-release-wp29-plenary-april-2017

3 Under these conditions, foreign companies are not able anymore to apply their local legislation. In case of infringement, the GDPR is much more threatening than existing regulations.

4 Dotted lines correspond to non-significant paths.

5 This effect was still not significant after removal of the ISS concern construct.

[6] Subgroups are smaller because values close to the average value of ISS concern were removed.

APPENDIX A: QUESTIONNAIRE AND DETAILED CONSTRUCTS

Constructs, References and Items		Code
Threat Appraisal (Vance et al., 2012; Siponen et al., 2014)		
Perceived severity		
If I lost my personal data, using my personal mobile device(s) to work there would be serious information security problems for me.		SEV1
If my personal data were temporarily not available because I work in BYOD-mode, serious problems would result for me.		SEV2
An information security breach, because I work in BYOD-mode would have a serious negative impact for my personal data.		SEV3
Perceived vulnerability		
An information security problem can occur for my personal data when I use my personal device(s) to work.		VULN1
My personal data can be subject to a threat when I use my personal device(s) to work.		VULN2
My personal data can be threatened when I use my personal device(s) to work.		VULN3
Information Security Concern (Malhotra et al., 2004; Kehr et al., 2015)		
In general, I am very concerned about threats to my personal information		ISC1
I am concerned that my personal information stored into my personal mobile device(s) for some reason, could be used for other reasons.		ISC2
I am concerned that my personal information stored into my personal mobile device(s) are not protected from unauthorized access.		ISC3
I am concerned about losing access to personal applications, through my lost or stolen personal mobile device(s).		ISC4 (*)
Control over personal mobile device(s) protection (Vance et al., 2012)		
I can implement data protection measures on my personal mobile device(s) by myself.		COSP1
Protecting my personal data on my personal mobile device(s) is easy for me.		COSP2
I have the capability to solve problems when I implement data security measures on my personal mobile device(s).		COSP3
Coping Strategies		
Disturbance handling (Beaudry and Pinsonneault, 2005; Workman et al., 2008; Tu et al., 2015)		
I regularly take measures to protect my personal mobile device(s) from personal information security issues.		DH1
I intend to take data protection measures to prevent others from getting my confidential data from my personal mobile device(s).		DH2
I intend to take measures to prevent unauthorized access to my personal mobile device(s).		DH3
Self-preservation (Beaudry and Pinsonneault, 2005; Workman et al. 2008; Moser et al, 2011)		
I do not take precautions against information security violations on my personal mobile device(s).		SP1 (*)
Potential risks of an everyday life will not affect my personal information or my personal mobile device(s).		SP2
I cannot do anything against information security risks related to mobile technologies.		SP3
Marker Variable: "Blue Attitude" (Simmering et al., 2015, p.491)		
I prefer blue to other colors.		MV1
I like the color blue.		MV2
I like blue clothes.		MV3
Control Variables		
Gender	M/F	GEND
Age	Number	AGE
Education	1: Self-taught; 2: NVQ1-2; 3: A level; 4: Higher education; 5 BA/BS; 6: MS/MA and higher	EDUC
Firm Size	Number	SIZE

(*) Items dropped: loadings < 0.7 leading to poor construct reliability and validity.

APPENDIX B: MEASUREMENT MODEL ANALYSES

Table 1. Construct reliability and validity and inter-construct correlations

Type	Constructs	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted	Disturbance Handling	Self-preserv.	Control device Protect	ISS Concern	Severity	Vulnerability
DVs	Disturbance Handling	0.833	0.882	0.895	0.741	**0.861**					
	Self-preservation	0.751	0.751	0.889	0.801	-0.164	**0.895**				
IVs	Control device Protect	0.887	0.908	0.929	0.814	0.490	-0.158	**0.902**			
	ISS Concern	0.900	0.952	0.936	0.829	0.212	-0.181	-0.038	**0.911**		
LOCs	Severity	0.868	0.868	0.919	0.791	0.069	-0.127	-0.092	0.308	**0.889**	
	Vulnerability	0.910	0.910	0.944	0.849	0.115	-0.200	-0.047	0.433	0.580	**0.921**

Squared root of AVE in bold, along the diagonal.
DVs: Dependent variables, IVs independent variables,
LOCs: Lower order constructs, forming the "Threat" higher order construct (HOC).

Table 2. Discriminant validity: HeteroTrait-MonoTrait ratio of correlations (HTMT)

Type	Constructs	Disturbance Handling	Self-preserv.	Control device Protect	ISS Concern	Severity	Vulnerability	Age	Educ.	Gender
DVs	Disturbance Handling									
	Self-preservation	0.212								
IVs	Control device Protect	0.517	0.213							
	ISS Concern	0.256	0.203	0.105						
LOCs	Severity	0.084	0.156	0.110	0.358					
	Vulnerability	0.139	0.243	0.096	0.483	0.652				
CVs	Age	0.023	0.093	0.103	0.118	0.065	0.030			
	Education	0.081	0.258	0.042	0.116	0.047	0.115	0.188		
	Gender	0.240	0.072	0.153	0.165	0.061	0.198	0.026	0.095	

CVs = Control variables

Table 3. Discriminant validity: Cross-loadings

	Disturbance Handling	Self-preserv.	Control device Protect	ISS Concern	Severity	Vulnerability
DH1	0.862	-0.111	0.587	0.092	0.044	0.065
DH2	0.859	-0.131	0.270	0.261	0.079	0.111
DH3	0.861	-0.192	0.314	0.245	0.064	0.139
SP2	-0.051	0.895	0.002	-0.201	-0.173	-0.248
SP3	-0.242	0.894	-0.286	-0.124	-0.055	-0.111
COSP1	0.503	-0.194	0.909	0.060	-0.052	0.026
COSP2	0.386	-0.104	0.886	-0.131	-0.149	-0.125
COSP3	0.419	-0.115	0.912	-0.062	-0.061	-0.052
ISC1	0.241	-0.175	0.032	0.914	0.188	0.347
ISC2	0.147	-0.073	-0.052	0.897	0.315	0.408
ISC3	0.169	-0.210	-0.099	0.920	0.365	0.442
SEV1	0.052	-0.073	-0.093	0.320	0.896	0.508
SEV2	0.025	-0.082	-0.070	0.197	0.881	0.498
SEV3	0.106	-0.182	-0.083	0.303	0.891	0.539
VULN1	0.106	-0.230	0.019	0.437	0.574	0.871
VULN2	0.101	-0.143	-0.062	0.383	0.526	0.945
VULN3	0.111	-0.181	-0.087	0.378	0.502	0.946

APPENDIX C: BOOTSTRAPPING RESULTS FOR PATH COEFFICIENTS

	Variable Influence (In bold: significant effects)	Path Coeff.	Sample Mean	Standard Deviation	Student's t-test	P Values
Direct effects	Threat -> Disturb. Handling	0.021	0.025	0.066	0.312	0.755
	Threat -> Self-preservation	-0.171	-0.171	0.074	2.308	0.021
	Control device Protect -> Disturb. Handling	0.465	0.463	0.066	7.019	0.000
	Control device Protect -> Self-preservation	-0.203	-0.202	0.088	2.308	0.021
	ISS Concern -> Disturb. Handling	0.219	0.222	0.064	3.446	0.001
	ISS Concern -> Self-preservation	-0.091	-0.099	0.074	1.226	0.220
Moderating effects	Control device Protect / Threat-> Disturb. Handling	-0.038	-0.036	0.056	0.683	0.495
	Control device Protect / Threat -> Self-preserv.	-0.030	-0.028	0.061	0.486	0.627
	ISS Concern / Threat -> Disturb. Handling	0.113	0.109	0.052	1.979	0.049
	ISS Concern / Threat -> Self-preserv.	0.060	0.055	0.063	0.950	0.342
Control variables	Age -> Disturb. Handling	-0.009	-0.008	0.050	0.181	0.857
	Age -> Self-preservation	0.043	0.043	0.067	0.636	0.525
	Educ -> Disturb. Handling	0.020	0.023	0.053	0.376	0.707
	Educ -> Self-preservation	-0.195	-0.196	0.061	3.211	0.001
	Gender -> Disturb. Handling	0.118	0.115	0.058	2.027	0.043
	Gender -> Self-preservation	0.107	0.106	0.063	1.701	0.089

APPENDIX D: SECOND-ORDER CONSTRUCT ASSESSMENT

Assessment of lower-order constructs (LOCs) forming the higher-order construct (HOC) "Threat":

1. As advised by Hair et al. (2018), both LOCs have an equal number of indicators;
2. The LOCs' internal consistency reliability is satisfactory (see Table 1 in Appendix B), as (1) all Cronbach's α values exceed 0.7, and (2) all composite reliability values are within the interval [0.7-0.95]. Average variance extracted (AVE) values are over 0.5, indicating good convergent validity for both constructs;
3. Both LOCs also satisfy discriminant validity (see Table 2 and Table 3 in Appendix B), between each other and other constructs, excluding the HOC they form: (1) All HTMT are smaller than 0.85 (2) the Fornell-Larcker criterion is met, as the square root of each construct's AVE exceeds the correlation with other constructs; and (3) indicators' loadings on each construct are higher than the cross-loadings with the other construct indicators' loadings;
4. The maximal variance inflation factor (VIF) value for the LOCs is 1.506, i.e., considerably below the threshold of 5, and therefore potential collinearity between the variables forming the HOC is not a critical issue for this model (Hair et al., 2018, p.62).

Assessment of LOCs weights and their significance for the HOC BYOD-related threat:

LOCs	Path Coeff.	Student's t-test	P Values	HOC
Severity -> Threat	0.529	30.728	0.000	Threat
Vulnerability -> Threat	0.596	27.298	0.000	

The LOCs weights correspond to the path coefficients between the LOCs and the reflective-formative HOC (Hair et al., 2018, p.55). They are strong, positive, highly significant and balanced (0.53 vs. 0.60), which is considered satisfactory (Hair et al., 2018).

APPENDIX E: COMMON METHOD BIAS ASSESSMENT

	Ctrl device protection	ISS Concern	Disturbance Handling	Self Preservation	Severity	Vulnerability	Marker variable
Ctrl device protection	1.000						
ISS Concern	-0.076	1.000					
Disturbance Handling	0.489	0.200	1.000				
Self Preservation	-0.180	-0.196	-0.177	1.000			
Severity	-0.091	0.385	0.085	-0.141	1.000		
Vulnerability	-0.041	0.472	0.116	-0.197	0.585	1.000	
Marker variable	0.082	0.079	0.048	-0.154	0.106	0.148	1.000

Highest squared correlation: $0.154^2 = 2.37\%$

APPENDIX F: COMPARISON BETWEEN THE PMT AND THE CMUA

The elements integrated in the research model (in Figure 6) are shown in gray.
The CMUA is based on the coping theory, which is "mute regarding what elements of a disruption are used in primary appraisal" (Beaudry & Pinsonneault, 2005, p. 498).
In this model, the primary appraisal is the threat appraisal, while the secondary appraisal is the coping appraisal. There is only one adaptation strategy, the protection motivation.
The two constructs added by Rogers (1983) permit an assessment of the threat appraisal that is missing from the CMUA.
Because it is exclusively problem-focused, the PMT does not permit an explanation of the self-preservation strategies (emotion-focused).

Figure 6. The coping model of user adaptation: adapted from Beaudry and Pinsonneault (2005)

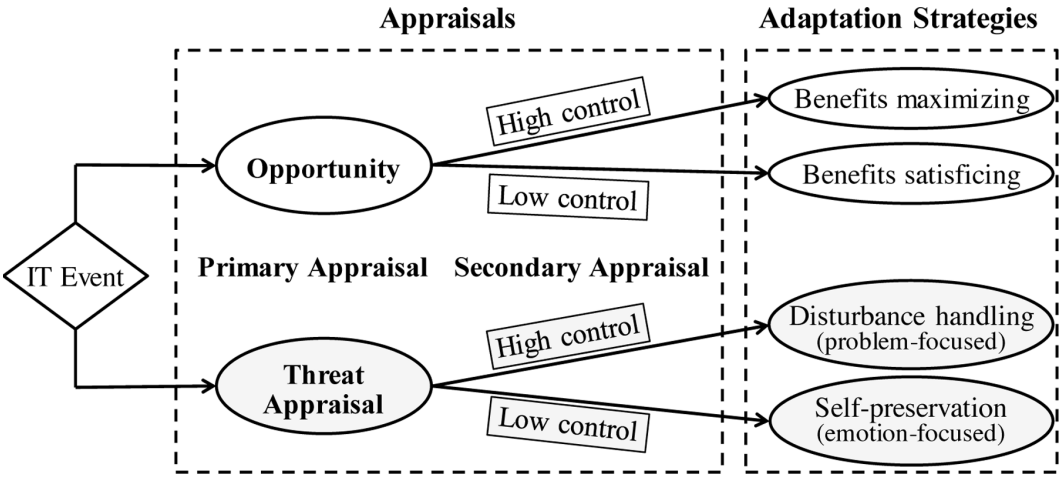
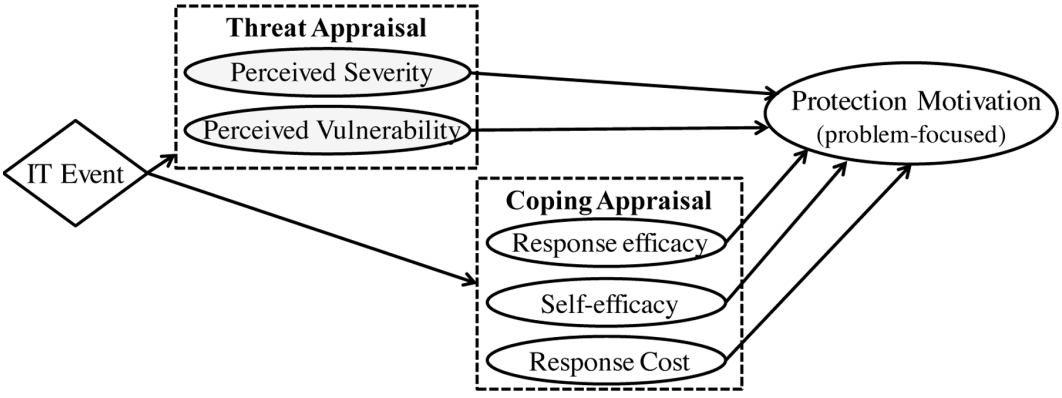


Figure 7. The protection motivation theory: Adapted from Rogers (1983)



Paméla Baillette is Associate Professor in Management Science-Information Systems at the University of Bordeaux, France. She is member of the research center IRGO-Bordeaux. Her current research interests include behavioral issues related to information security, technological and management innovation, and traceability related to agribusiness management. She has published research papers in International Journal of Information Management, Systèmes d'Information et Management, Revue Internationale P.M.E., Journal of Organizational Change Management, and International Small Business Journal.

Yves Barlette is Full Professor of Information Systems at Montpellier Business School, France. He is member of the MRM research center and Entrepreneurship & Innovation Chair, part of LabEx Entrepreneurship. His current research interests include behavioral issues related to information security in SMEs, and on the digital transformation of organizations. He has published research papers in Systèmes d'Information et Management, International Journal of Information Management, Production Planning & Control. He also authored thirteen books and book chapters. Yves Barlette is the corresponding author and can be contacted at: y.barlette@montpellier-bs.com