Examining CEOs' behavior related to BYOD implementation through the CMUA

Paméla Baillette, Yves Barlette

AiM
MONTRÉAL 2018

Paméla Baillette*
Yves Barlette**
MRM, Montpellier Research in Management
* Université de Perpignan Via Domitia, France
** Montpellier Business School, France

Examining CEOs' behavior related to BYOD implementation through the CMUA

Abstract:

Despite prior research on the 'Bring Your Own Device' (BYOD) phenomenon, little attention has been paid to perceptions of opportunities/threats associated with the implementation of BYOD by CEOs. This quantitative study is based on the coping model of user adaptation (CMUA). We enriched this model with quantitative constructs for assessing the CEOs' beneficial and threatening perceptions of BYOD implementation. We also added CEOs' information security (ISS) concern, in order to identify potential security paradoxes, i.e., discrepancies between their concerns and the adopted coping strategies. Results indicate that perceived opportunities/threats and perceived behavioral control have an impact on the type of coping strategy adopted. This study clarifies the operationalization of an enriched CMUA and offers managerial contributions regarding improved protection of corporate information when implementing BYOD. These are the first results concerning 61 CEOs. The full results will be released during the AIM conference with 200+ responses in May 2018.

Keywords:

BYOD, CMUA, CEO, Security paradox, Coping, Behavior.

1. Introduction

The BYOD phenomenon, i.e. 'Bring Your Own Device', is growing in businesses and increasingly affecting CEOs. It refers to the provision and use of personal mobile devices (smartphones, tablets or laptops) by employees for both private and business purposes. Even if this way of working takes on many opportunities, such as organizational cost savings (Steelman et al., 2016), increased process performance (Zhou et al., 2010) and productivity gains (Leclercq-Vandelannoitte, 2015; Steelman et al., 2016), it creates additional security breaches resulting in higher risks for companies.

The perception of opportunities and threats and the resulting coping behaviors can be assessed through the CMUA, that is, the coping model of user adaptation (Beaudry & Pinsonneault, 2005, 2010). The CMUA has been successfully used to identify coping behaviors related to the adaptation and use of technologies, and states that after a primary appraisal corresponding to the perception of an event as threatening of beneficial, a second appraisal – based on perceived behavioral control – leads to the adoption of a coping behavior that can be problem-focused (high control over the situation, mainly leading to actions) or emotion-focused (low control, leading to passivity or denial, for example). However, while this model has been quantitatively tested and validated for the second appraisal (Elie-Dit-Cosaque & Straub, 2011), to date, there has been no assessment of the primary appraisal using quantitative constructs[1].

Previous research has mainly focused on individuals and highlighted several factors determining the adoption of mobile tools by employees (Weeger et al., 2016). In a BYOD context, research has chiefly focused on threats to employees' privacy (Pentina et al., 2016) or employee compliance with information security (ISS) policies (Hovav & Putri, 2016). Less attention has been paid to the perception by CEOs of opportunities and/or threats related to BYOD implementation, and the resulting behaviors.

We aim at contributing to current research by (1) complementing the CMUA with constructs permitting (2) to assess CEOs' perceived threats and opportunities (3) in the specific context of BYOD. In addition, while problem-focused strategies (i.e., 'active' behaviors), are often examined, emotion-focused strategies (i.e., 'passive' behaviors) remain under-researched. Using the CMUA framework will offer insights on CEOs problem-focused and emotion-focused strategies and will permit to compare the influence of their determinants.

The CMUA offers a last advantage: as it allows us in a same model to assess the benefits and threats of BYOD for CEOs, it provides a good basis to examine security paradoxes. In our context, a security paradox can occur when the perception of BYOD advantages outweighs the risks involved, organizations endanger their data by authorizing or encouraging users to work in BYOD mode without implementing sufficient security measures, despite a strong assertion of their concerns about data security (Baillette & Barlette, forthcoming). Therefore, complementing the CMUA model with the construct "information security concern" will permit to identify potential security paradoxes related to the implementation of BYOD in companies.

The next section reviews the relevant literature, the third section explains how we complement the CMUA framework and our hypotheses. Following the methodological section, the fifth

[1] Elie-Dit-Cosaque and Straub (2011) used scenarios to assess the primary appraisal.

section presents our current results. After a short discussion, the conclusion reviews the current state of our research.

2. Literature review

Beaudry and Pinsonneault (2005) built the coping model of user adaptation (CMUA), on the Lazarus' (1966) coping theory. 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). Coping theory states that certain events can trigger adaptive behaviors based on two key sub-processes. The *primary appraisal* consists in evaluating the potential consequences of the event (threats, opportunities or both) and its personal significance (Folkman, 1992). The *secondary appraisal* is the evaluation of the coping options available and corresponds to *coping efforts,* either *problem* or *emotion-focused*, depending on the degree of individual's perceived control over the situation. Beaudry and Pinsonneault (2005) have adapted the coping theory to IT events, as most IT events can be appraised as both opportunities and threats. Further studies have since confirmed the insights offered by the CMUA (Beaudry & Pinsonneault, 2010; Elie-Dit-Cosaque & Straub, 2011).

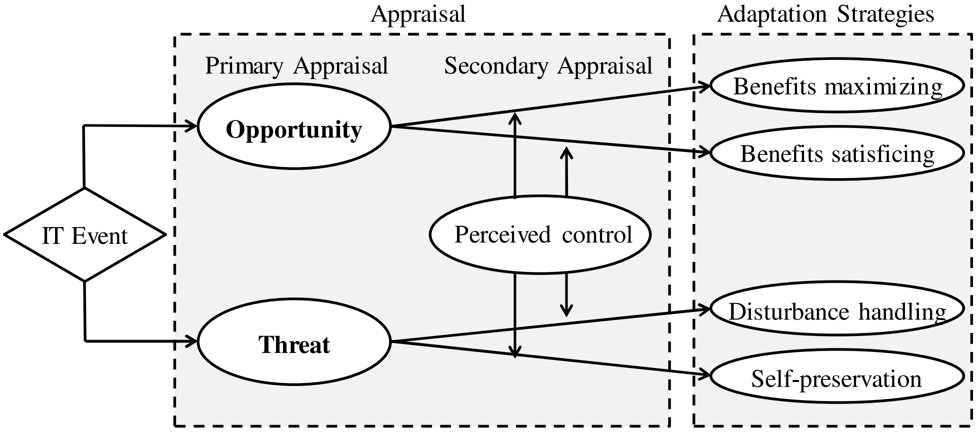


Figure 1. The CMUA model. Adapted from Beaudry & Pinsonneault (2005).

The next subsections deal with the primary and secondary appraisals characterizing coping behaviors. The third subsection introduces the "information security concern" that may allow identification of security paradoxes.

2.1 Primary Appraisal

The CMUA is based on coping theory, which is "*mute regarding what elements of a disruption are used in primary appraisal*" (Beaudry & Pinsonneault, 2005, p. 498). Therefore, to enable an assessment of this primary appraisal, i.e., threatening and beneficial events, we complemented the CMUA by adding constructs borrowed from previous research.

2.1.1 Threat Appraisal

Threat related to BYOD implementation and usage is assessed through two constructs, adapted from another coping-based theory, i.e., the Protection Motivation Theory (PMT) (Rogers, 1983). The constructs permitting to assess the first appraisal (threat appraisal) are the individual's *perceived vulnerability* (e.g., the probability) of the potential event and the individual's *perceived severity* (e.g., the impact) when the event materializes (see Figure 2).

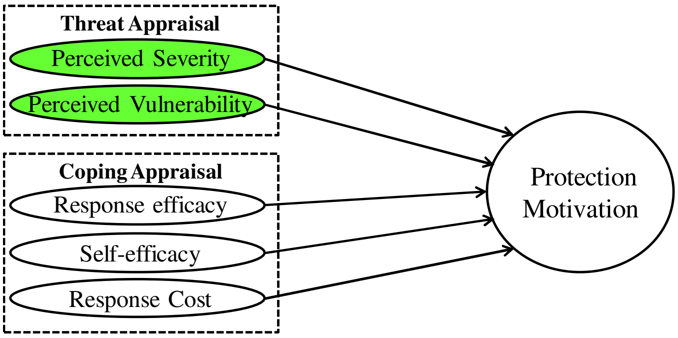


Figure 2. The PMT – Threat appraisal. Adapted from Rogers (1983).

Perceived vulnerability is the probability of occurrence of a threatening event, provided that no adaptive behavior is performed or there is no adaptation of an existing behavior (Lee & Larsen, 2009). *Perceived severity* is the perceived impact of an ISS problem, due to insufficient or ineffective ISS measures (Liang & Xue, 2009). In our model, these two construct will represent the underlying formative dimensions of the threat appraisal (See Figure 3).

2.1.2 Opportunity Appraisal

Benefits of BYOD include increased productivity and innovation for the company (Tu & Yuan, 2015). For organizations, benefits are ranging from organizational cost savings (Steelman et al., 2016) to individual task efficiencies and productivity gains (Leclercq-Vandelannoitte, 2015; Steelman et al., 2016). Therefore, we define the perceived benefits for a CEO to implement BYOD in his/her company as the combination of *Business process improvement* (Law & Ngai, 2007), *Cost advantages* (Benlian & Hess, 2011) and *Performance expectancy*, (Moore & Benbasat, 1991; Venkatesh et al., 2003, p. 449).

Business process improvement involves the simplification and improvement of work practices and processes through re-engineering (Law & Ngai, 2007, p. 422). BYOD can deliver tangible benefits such as business process improvement (Leclercq-Vandelannoitte, 2015). Kim et al. (2017) showed that business process improvement was significantly related to perceived opportunity. *Cost advantages:* Many executives seek to leverage the potential benefits of BYOD, such as cost savings (Steelman et al., 2016). Allowing employees to use their personal device for corporate purposes contributes to a reduction of investment costs via the private procurement of devices. Further cost savings can be achieved via an external storage of corporate data (Weiss & Lemeister, 2012). Free or low-cost mobile applications “apps” are increasingly integrated into corporate infrastructure (Weiss & Lemeister, 2012). In their research, Benlian and Hess (2011) considered cost advantage as the strongest and most consistent factor affecting perceived opportunities. Performance expectancy is defined as "*the degree to which using an innovation is perceived as being better than using its precursor.*" (Moore & Benbasat, 1991, p. 196). These three constructs are the underlying formative dimensions of the opportunity appraisal (See Figure 3).

This primary appraisal (e.g., opportunity or threat) entails a secondary appraisal, consisting of emotion-focused and problem-focused strategies (Beaudry & Pinsonneault, 2005; Lazarus & Folkman, 1984).

2.2 Secondary appraisal and the four adaptation strategies

The CMUA postulates (See Figure 1) that four coping strategies can be adopted, depending on the perception of the situation and the perceived behavioral control by the individual (Beaudry & Pinsonneault, 2005, 2010). A high level of perceived behavioral control over coping behavior will lead to problem-focused coping strategies (*benefits maximizing* and *disturbance handling*), while a low level of perceived behavioral control will lead to more passive (emotion-focused) coping strategies (*benefits satisficing* and *self-preservation*). Table 1 below summarizes these four coping strategies.

Secondary appraisal Primary appraisal	Low control Emotion-focused	High control Problem-focused
Opportunity	Benefits Satisficing	Benefits Maximizing
Threat	Self-Preservation	Disturbance Handling

Table 1. Effect of perceived control on the coping strategies of user adaptation
(adapted from Beaudry & Pinsonneault, 2005)

The *benefits satisficing* strategy corresponds to the use of minimal problem-focused efforts: first, as the situation is perceived as beneficial, there is no actual need to act, and second, as the perceived control is low, the reaction will be mainly emotion-focused. Moreover, as no tensions emanate from the IT event, there is no need to reduce them. Therefore, CEOs will rather passively enjoy the beneficial situation, as they are satisfied with a status quo.

The *benefits maximizing* strategy occurs when CEOs perceive the IT event as an opportunity and when their perceived control over the situation is high. In such a case, their problem-focused coping strategy aims at maximizing the benefits offered by the IT event. For example, CEOs can focus on increasing their productivity, reducing costs, increase their revenues, benefits from new processes, etc.

The *self-preservation* strategy corresponds to situations wherein CEOs perceive potential threats but have limited control. The coping strategy they use to reduce the tensions emanating from the IT event is emotion-focused. Six types of adaptation efforts can be adopted: minimization of consequences, passive acceptance, denial, selective attention, positive comparison and distancing.

The *disturbance handling* strategy corresponds to CEOs appraising a threatening situation and having control over this situation. CEOs' coping efforts will mainly be problem-focused, and they will act to prevent the occurrence of the negative event (e.g., implementing protective measures).

2.3 From Information Security Concern to Security Paradoxes

The main danger of BYOD for CEOs is related to their company's *information security,* which corresponds to the preservation of the information confidentiality, integrity and availability. Information *confidentiality* reflects CEOs' desire to avoid disclosure of their corporate information to undesired third parties (Hong & Thong, 2013). *Integrity* problems include cases when certain types of information are damaged or even erased. *Availability* issues correspond to situations in which information access is impossible. Previous research has shown that CEOs perform a balance between the perceived disadvantages and benefits of enjoying mobile technologies (Keith et al., 2013). Hence, CEOs face a dilemma to protect their information or to enjoy the benefits provided by mobile tools and apps. However, they allow their employees to bring their own devices by favoring benefits over security concerns (Dinev & Hart, 2006). Therefore, if the perceived benefits are sufficient, CEOs can overlook the dangers arising from the risks they agree to take (Keith et al., 2013; Sutanto et al., 2013), leading to security paradoxes. Security paradox situations were defined in the introduction of this paper as an imbalance between the protective action implemented and the increased risks stemming from the implementation of a technology involving benefits (i.e., BYOD in our case), despite the expression of high security concerns.

3. Hypothesis development and Conceptual Model

3.1. Primary appraisal: opportunity and threat

3.1.1 Influence of perceived opportunity on Benefits Maximizing and Benefits Satisficing

Previous research in I.S. showed that the perceived benefits are positively associated with the use of information technologies and applications (Benlian & Hess, 2011; Elie-Dit-cosaque & Straub, 2011; Kim et al., 2017; Moore & Benbasat, 2011). In the context of smartphones, previous studies confirmed that a high perception of BYOD-related benefits favored smartphone adoption and usage (Kim et al., 2013). Consequently, we propose:

- H1a-b: *The perception of a BYOD-related opportunity will positively influence the adoption of (a) Benefits Maximizing and (b) Benefits Satisficing strategies.*

3.1.2 Influence of perceived threat on Disturbance Handling and Self-preservation

Theories addressing coping behaviors, such as protection motivation theory (PMT) (Rogers, 1983), have been adapted to the ISS context (Lee & Larsen, 2009; Siponen et al., 2014; Vance et al., 2012). Several studies adapted these theories to smartphone security (Tu et al., 2015) and smartphone-related threats (Weeger et al., 2016; Whitten et al., 2014). Previous research showed that the perception of an event as a threat (Siponen et al., 2014; Vance et al., 2012) leads CEOs to behave in a more cautious manner (Bulgurcu et al., 2010). Weeger et al. (2016) showed that individuals fear that a BYOD program may harm their data. In the context of mobile devices, the perception of this threat is positively associated with the intention to implement countermeasures (Tu et al., 2015). Therefore, we propose:

- H2a-b: *The perception of a BYOD-related threat will positively influence the adoption of (a) Disturbance Handling and (b) Self-preservation strategies.*

3.2. Secondary appraisal: influence of Perceived Behavioral Control

The research model in Figure 3 provides an overview of the hypotheses. We hypothesized that the perceived behavioral control can exert two kinds of effects on the coping behavior, i.e., direct, according to PMT-based studies and moderating, according to the CMUA. Consequently, hypotheses 3-4 were added to address direct effects and hypotheses 7-8 were added to address potential moderating effects, similar in strength and direction (Figure 3).

3.2.1. Perceived Control over BYOD implementation

This variable refers to "*how much influence users feel they have over the features and functionalities of the IT*" (Beaudry & Pinsonneault, 2005, p. 500). When perceived control is high, for instance, people apply their IT competence to achieve better performance (Beaudry & Pinsonneault, 2005; Harris et al., 2012). CEOs with high perceived control will mainly adopt problem-focused responses (Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011). Conversely, when CEOs perceive that they have low control over the situation, they will mainly adopt an emotion-focused coping strategy (See Table 1). Hence, we propose:

- H3a-b (direct effect): *When CEOs appraise the situation as an opportunity, the more perceived control they have over benefitting from BYOD, (a) the more inclined they will be to adopt a benefits maximizing strategy and (b) the less inclined they will be to adopt a benefits satisficing strategy.*
- H7a-b (moderating effect): *When CEOs appraise the situation as an opportunity, the level of perceived control they have over benefitting from BYOD will moderate (a) positively the relationship between the BYOD-related opportunity and the benefits maximizing strategy and (b) negatively the relationship between the BYOD-related opportunity and the benefits satisficing strategy.*

3.2.2. Perceived Control over BYOD-related security measures implementation

This variable corresponds to "*the degree that the individual believes it is possible to implement the protective behavior*" (Vance et al., 2012, p.190), which, in this study, refers to implementing data protection measures in the company. When a situation is perceived as threatening, the protection motivation becomes stronger and results into two alternatives (Moser et al., 2011): high levels of perceived control over information protection are associated with threat-reducing actions, while, when no behavior alternative is perceived as reliable, people choose emotion-focused, e.g., non-protective responses. Prior research has found that increased threat appraisal, as well as increased coping efficacy, intensified the protective responses (Moser et al., 2011). Consequently, the following hypotheses are proposed:

- H4a-b (direct effect): *When CEOs appraise the situation as a threat, the more perceived control they have over information 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.*
- H8a-b (moderating effect): *When CEOs appraise the situation as a threat, the level of perceived control they have over information protection will moderate (a) positively the relationship between the BYOD-related threat and the disturbance handling strategy and (b) negatively the relationship between the BYOD-related threat and the self-preservation strategy.*

3.3. Influence of information security concern and security paradoxes

Information security concern was added in order to identify potential security paradoxes by juxtaposing the CEOs' expressed information security concern with their primary appraisal (beneficial or threatening) and the appropriateness of their adopted coping strategies.

3.3.1. Hypotheses on the effect of information security concern

Previous literature showed that concern about potential information loss of confidentiality negatively affects the extent of adopting mobile apps (Pentina et al., 2016), and the adoption intention to use e-commerce or personalization services (Dinev & Hart, 2006; Guo et al., 2016; Li & Unger, 2012; Sutanto et al., 2013). In other studies, information privacy concern was also found to exert a negative moderating role on the relationship between the perception of a benefit and continuance intention to use social network services (Ku et al., 2013).

Consequently, we hypothesize that information security concern can exert direct and/or moderating effects. Hypotheses 5-6 were added to address direct effects, while hypotheses 9-10 were added to address moderating effects (see Figure 3). Therefore, we propose:

- H5a-b (direct effect): *When CEOs appraise the situation as beneficial, their information security concern will exert a negative effect, (a) on the adoption of a benefits maximizing strategy and (b) on the adoption of a benefits satisficing strategy.*
- H9a-b (moderating effect): *When CEOs appraise the situation as beneficial, the level of their information security concern will exert a negative moderating effect (a) on the relationship between the BYOD-related opportunity and the benefits maximizing strategy and (b) on the relationship between the BYOD-related opportunity and the benefits satisficing strategy.*

Previous literature showed that individuals with higher privacy concern were found to adopt more restrictive privacy settings (Utz & Krämer, 2009) and to adopt more protective behaviors and privacy policy consumption (Stutzman et al., 2011). Consequently, we propose:

- H6a-b (direct effect): *When CEOs appraise the situation as a threat, a higher information security concern will exert (a) a positive effect on the adoption of a disturbance handling strategy and (b) a negative effect on the adoption of a self-preservation strategy.*
- H10a-b (moderating effect): *When CEOs appraise the situation as a threat, a higher level of their information security concern will exert (a) a positive moderating effect on the relationship between the BYOD-related threat and the disturbance handling strategy and (b) a negative effect on the relationship between the BYOD-related threat and the self-preservation strategy.*

3.3.2. Information security concern and identification of potential security paradoxes

When CEOs perceive an event as beneficial, information security concern should not have any direct or moderating effect on the choice between benefits maximizing and benefits satisficing strategies. According to the CMUA, perceived control should be the only factor influencing this choice. Table 2 summarizes the expected effects of information security concern on coping strategies and the potential occurrence of security paradoxes.

Coping Strategy	Effect of higher information security concern on potential security paradox
Benefits maximizing	If positive effect.
Benefits satisficing	If positive effect.
Disturbance handling	If no effect or negative effect.
Self-preservation	If no effect or positive effect.

Table 2. Information security concern and potential security paradox

Other paradoxes could be identified if there is no significant impact of behavioral control on protective strategies or if specific subgroups with abnormal behaviors can be established.

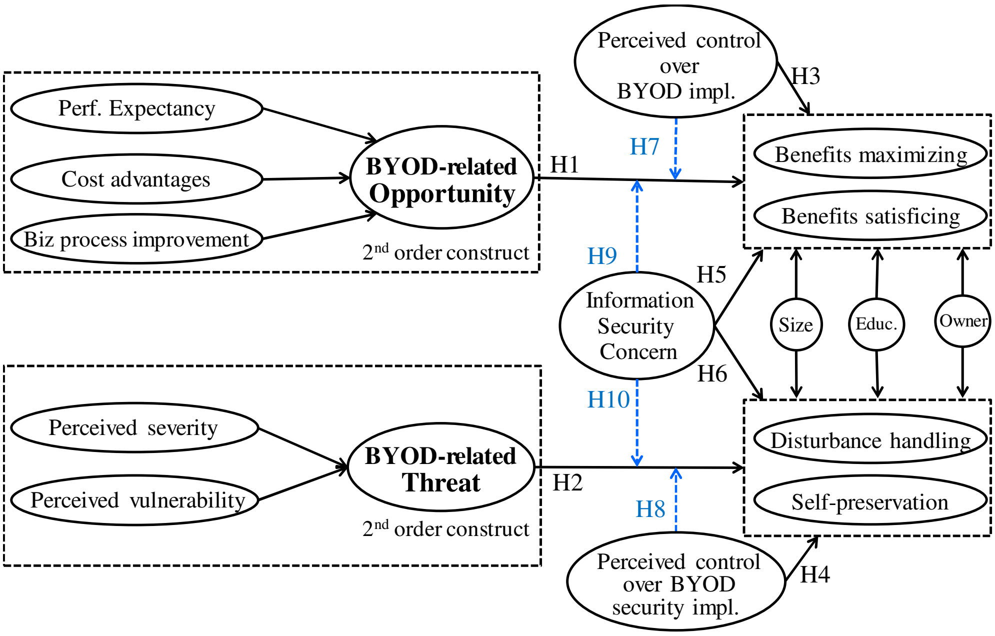


Figure 3. Research model (dotted arrows: moderating effects)

4. Research Method

4.1 Research Design

In order to determine the coping behaviors stemming from the CEOs' perception of BYOD implementation and the possible occurrence of security paradoxes, we conducted a questionnaire-based survey. The details of the variables and items used in the questionnaire can be found in Appendix. 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 CEOs (N=12). 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. An introductory section of the questionnaire 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.

We included a link to this questionnaire in an email presenting our survey. This survey involved CEOs willing to implement or having implemented BYOD in their company. The questionnaire was administrated through business school alumni and companies from various incubators, during November 2017. A total of 74 responses were collected. After removing incomplete and invalid responses, 61 usable responses were obtained. The collected data were analyzed using SmartPLS 3.2.7.

4.2. Construct operationalization and measures

In order to reduce the number of relationships in our structural model and make it more parsimonious and easier to apprehend (Hair et al., 2018, p.40), we modelled the first appraisal though two second-order reflective-formative constructs (Hair et al., 2017b). Higher-order constructs are better predictors of broadly defined behaviors, and they overcome the jangle fallacy (Hair et al., 2018).

Hence, *BYOD-related opportunity* was operationalized as a second order construct composed of three constructs: business process improvement, cost advantages and performance expectancy. *BYOD-related threat* was operationalized as a second order construct composed of perceived severity and perceived vulnerability (Figure 3).

The questionnaire and the scales used in this study (see Appendix 1) were adapted from previously validated research:

- The *Business process improvement* (BPI) scale was adapted from Law & Ngai, (2007), *Cost advantages* (CA) scale comes from Benlian and Hess (2011) and *Performance expectancy* (PERF) was borrowed from Moore & Benbasat (1991).
- The *perceived severity* (SEV) and *perceived vulnerability* (VULN) scales used measures adapted from Vance et al. (2012) and Siponen et al. (2014);
- The *information security concern* (ISC) scale was adapted from Malhotra et al. (2004);
- The scales corresponding to the four coping strategies were mainly borrowed from Beaudry and Pinsonneault (2005), Elie-Dit-Cosaque and Straub (2011) and Workman et al. (2008).

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

Three control variables (CVs) were included in the model: *Owner* (OWNER) was included in the form of a dummy variable (Non-owner=0; Owner=1). *Size* (SIZE) represents the company's size; *Education* (EDUC) is detailed in appendix A.

5. Data Analysis and first Results[2]

To validate the measurements and test hypotheses, we used Partial Least Squares Structural Equation Modeling (PLS-SEM) analyses. This 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, PLS-SEM is "*virtually without competition*" (Richter et al., 2016).

5.1. Descriptive statistics

The average CEOs' age is 41 years old. The proportion of male vs. female CEOs is 75/25 percent. The sample mainly contained SMEs (27 very small, 11 small, 4 medium enterprises) and only 2 large enterprises. We expect larger companies in our extension of the study.

5.2. Model Assessment

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 standardized root mean square residual (SRMR): value of 0.117 slightly exceeds the threshold of 0.100 for the estimated model (Hair et al., 2017b).

Measurement Model Analysis

Indicator Reliability and Constructs' Internal Consistency Reliability (See table B1 in Appendix B)*:* All composite reliability values are within the interval [0.7-0.95], meeting the "satisfactory to good" condition (Hair et al., 2017b). All AVE (average variance extracted)

[2] Due to page count restrictions and as additional responses are expected, only some results are reported in appendixes. Our full results will be provided for the AIM conference.

values but one are over 0.5, indicating good convergent validity of the constructs (Henseler et al., 2016).

Discriminant Validity

See tables B1-B2 in Appendix B. For each construct, the squared root of the AVE exceeds the highest correlation with other constructs. Hence the Fornell-Larcker criterion is met (Fornell & Larcker, 1981). All heterotrait-monotrait ratios of correlations (HTMT) are smaller than 0.90 (Henseler, Ringle & Sarstedt, 2015, 2016), exhibiting acceptable discriminant validity.

Reflective-formative second order constructs assessment:

All tests exhibit satisfying results (see Tables B3 in Appendix B).

5.3. Structural Model Analysis

Figure 4 shows the current R² (N=61). The bootstrapping test provided the estimates of standard errors for testing the statistical significance of the path coefficients using t-tests and p values. Our first results still lack significance for now as they solely represent 61 responses. However, some results are already salient while other are promising. When BYOD is perceived as beneficial, it influences positively (β=0.56***) the *benefits maximizing* strategy (R²= 0.61). Information security concern could also moderate positively and reinforce this influence (β=0.47°). There is a hint for a smaller positive influence (β=0.29°) on the benefits satisficing strategy (R²= 0.43). The perception of a threatening event will strongly influence (β=0.52**) the disturbance handling behavior (R²= 0.44) while strongly negatively (β=-0.54**) influencing the self-preservation coping strategy (R²= 0.50). Information security concern exerts a positive and significant direct influence (β=0.29*) on the disturbance handling coping strategy. For now, the perceived behavioral control does not exert any significant influence, neither direct nor moderating.

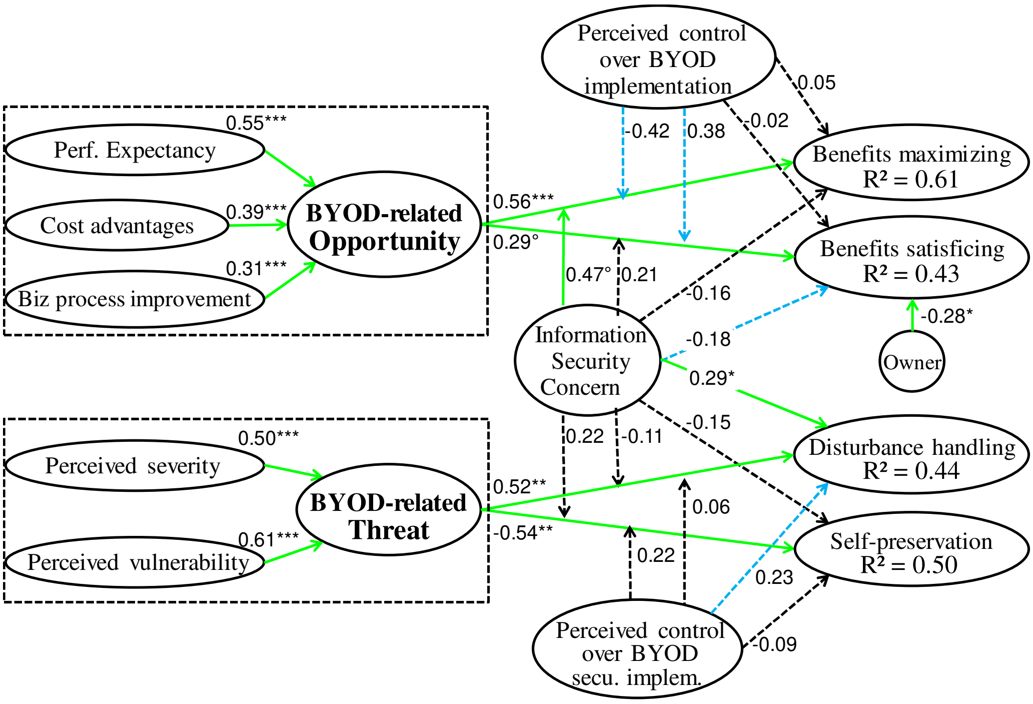


Figure 4. Results and significance of path coefficients[3]

**** p<0.001, ** p<0.01, * p<0.05, ° p < 0.16* [4]

[3] Dotted lines correspond to non-significant paths. Only the significant relationships are shown for CVs.

[4] '°' These p values were tolerated while expecting additional results by May 2018.

5.4. Common Method Bias Assessment

The survey data were self-reported and behavior was self-assessed by respondents and was not actually measured (Straub *et al.*, 1995). Consequently, our results can potentially be confounded by common method bias (Podsakoff *et al.*, 2003). Hence, we used several means of assessing and minimizing the potential common method bias. First, we used the recommended a priori procedural remedies (Podsakoff *et al.*, 2012), such as improvements to scale items through pretests to reduce potential ambiguities, as well as breaking the routine of Likert scales with 'yes/no' or multiple choice questions. Second, we applied the correlational technique (Lindell & Whitney, 2001): Its assessment of the extent to which CMV may be biasing the results of PLS-SEM studies has been validated by Malhotra et al. (2015). For that purpose, we included in our model (Simmering et al., 2015) an a priori 'ideal' marker variable (MV), the "blue attitude", (the three items can be found in Appendix A) theoretically uncorrelated with other variables included in the model. Our results demonstrate that the average correlation between the marker variable and the latent factors included in the model does not exceed 3.47%, well below the threshold of 9% (Tehseen *et al.*, 2017). Third, the results of the structural model showed different levels of significance for the path coefficients. For these reasons, CMV bias is unlikely to be a serious concern in our study.

6. Discussion

6.1 Interpretation of Results (N=61)

Table 3 below highlights the main effects observed and the validation of hypotheses.

6.1.1 Effects of Perceived behavioral Control

For *perceived control over BYOD implementation*, some important beta values begin to appear, while still not significant. For a beneficial event, a moderating effect could appear, but counterintuitive: being negative (β=-0.42) for the benefits maximizing strategy and positive (β=0.38) for the benefits satisficing strategy. No direct effects were identified. When addressing *perceived control over information security measures implementation*, the most important beta is a direct effect on the disturbance handling strategy (β=0.23). No moderating effects were identified.

	# Hyp.	Variable Influence	Beta	T Statistics	P Values	Hyp Validation
Direct Effects	1a	Opport -> Benef Max	0.560	5.201	0.000	Yes
	1b	Opport -> Benef Sat	0.286	1.418	0.157	Possible (*)
	2a	Threat -> Disturb Handl	0.519	3.101	0.002	Yes
	2b	Threat -> Self Preserv	-0.539	3.255	0.001	Yes
	3a	Control Implement -> Benef Max	0.052	0.445	0.656	No
	3b	Control Implement -> Benef Sat	-0.024	0.113	0.910	No
	4a	Control Protect -> Disturb Handl	0.230	1.271	0.204	Possible (*)
	4b	Control Protect -> Self Preserv	-0.087	0.638	0.524	No
	5a	InfoSec Concern -> Benef Max	-0.159	1.108	0.268	No
	5b	InfoSec Concern -> Benef Sat	-0.181	1.206	0.228	No
	6a	InfoSec Concern -> Disturb Handl	0.287	1.961	0.049	Yes
	6b	InfoSec Concern -> Self Preserv	-0.146	0.756	0.450	No
Moderating Effects	7a	Control Impl Opport -> Benef Max	-0.423	1.151	0.250	Possible (*)
	7b	Control Impl Opport -> Benef Sat	0.381	1.137	0.256	Possible (*)
	8a	Control Prot Threat -> Disturb Handl	0.057	0.203	0.839	No
	8b	Control Prot Threat -> Self Preserv	0.218	0.996	0.319	No
	9a	InfoSec Concern Opport -> Benef Max	0.465	1.564	0.118	No/Paradox (*)
	9b	InfoSec Concern Opport -> Benef Sat	0.206	0.708	0.479	No
	10a	InfoSec Concern Threat -> Disturb Handl	-0.114	0.680	0.497	No
	10b	InfoSec Concern Threat -> Self Preserv	0.217	1.079	0.281	No

Table 3. Effects and Hypotheses validation

(*) These effects could become significant when more data is collected

6.1.2 Effects of Threat and Opportunity Appraisals

Perceived opportunity (H1a, β=0.56***) influences the adoption of benefits maximizing strategies, and possibly influences (H1b, β=0.29°) the benefits satisficing strategy. Perceived threat has the same but opposite strength of effect on the adoption of disturbance handling strategies (H2a, β=0.52**) and (H2b, β=-0.54**).

6.1.3 Effects of Information Security Concern

InfoSec Concern exerts only one direct effect on the disturbance handling strategy (H6a, β=0.29*). For the probable effects, a positive moderating effect could exist, thus reinforcing the relationship between the perception of a BYOD-related opportunity and the benefits maximizing strategy. This could lead to a security paradox. InfoSec Concern could also have a negative direct effect on the benefits satisficing strategy (H5b, β=-0.18).

As hypothesized for H5a and H9b, in these cases InfoSec concern had no influence on coping strategies related to positive appraisals.

6.1.4 Effects of Control Variables

The only effect identified was related to the ownership of the company, negatively influencing the benefits satisficing strategy (β=-0.28). Owners are more likely to be just satisfied with the implementation of BYOD. This counterintuitive and interesting result has already been identified by Barlette et al. (2017). Multigroup analyses will be performed when we reach our goal of 200+ responses.

6.2 Theoretical Contributions

This research offers several theoretical contributions. Very little work has been published in the field of information systems about the benefits and risks associated with CEOs' BYOD-related practices. This paper is the first to aim at identifying CEO's information security paradox related to BYOD implementation.

Second, this paper models and operationalizes the CMUA through structural equations and extends it via several exogenous latent variables. The CMUA was extended to beneficial appraisals with constructs adapted from Moore and Benbasat (1991) and Kim et al. (2017) and to threatening appraisals by constructs borrowed from the PMT (Rogers, 1983; Siponen et al., 2014; Vance et al., 2012). The 'perceived control over behavior' construct was operationalized with moderated and direct effects: some results are promising in obtaining insights regarding how to operationalize this construct in future research.

Third, this study shows that information security concern can exert effects on the adopted coping behaviors. In the field of information security, this concern deserves more inclusion in models addressing coping behaviors.

6.3 Managerial Contributions

This study intended to identify how BYOD can be perceived by CEOs through their appraisal of BYOD, as an opportunity or a threat. Identifying security paradoxes, i.e., an overlook of threats to benefit from the BYOD-related perceived opportunities, would allow to build countermeasures. 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 behaviors corresponding to denial – "*Risks will not affect me*"– and distancing –

"*I cannot do anything*" (see Appendix). This would also enhance disturbance handling behaviors, resulting in higher information security for CEOs and their companies. Even if CEOs are not specialists, they could provide more funding for security measures, or support the implementation of charters, training sessions or awareness raising campaigns.

7. Conclusion

This study applied the CMUA to the context of information protection related to BYOD practices. The CMUA was enriched with constructs allowing the assessment of beneficial and threatening situations. Perceived behavioral control was modeled as having potential direct and moderating effects. Information security concern was also added to the model to identify security paradoxes.

Our first results are based on 61 responses. We will provide more reliable results for the AIM conference, as our goal is to obtain 200+ responses by May 2018. No security paradoxes could be identified for the moment, but we remain confident, as we could identify paradoxes in another study addressing employees' BYOD-related behaviors through the CMUA.

Funding: This research received financial support from the French National Research Agency through the program 'Investments for the future' under reference number ANR-10-LabX-11-01.

References

Baillette, P., & Barlette, Y. (forthcoming), BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: the identification of a twofold security paradox. *Journal of Organizational Change Management*.

Barlette Y., Gundolf K., & Jaouen A. (2017), CEOs' Information Security Behavior in SMEs: Does Ownership Matter? *Systèmes d'Information et 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 Executives. *Decision Support Systems*, 52(1), 232-246.

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.

Dinev, T., & Hart, P. (2006), An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

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.

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. *Journal of Marketing Research*, *18*(1), 39-50.

Guo, X., Zhang, X., & Sun, Y. (2016), The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications*, 16, 55-65.

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.

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: Sage.

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

Hong, W., & Thong, J. (2013), Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275-298.

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.

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.

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.

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 and Management*, 44(4), 418-432.

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 Company.

Leclercq-Vandelannoitte, A. (2015), Leaving employees to their own devices: new practices in the workplace. *Journal of Business Strategy*, 36(5), 18-24.

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.

Li, T., & Unger, T. (2012), Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, 21, 621-642.

Liang, H., & Xue, Y. (2009), Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71-90.

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.

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.

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.

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.

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.

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.

Richter, N.F., Cepeda, G., Roldán, J.L., & Ringle, C.M. (2016), European management research using partial least squares structural equation modeling (PLS-SEM). *European Management Journal*, *34*(6), 589-597.

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* (p. 153-176). New York: Guilford Press.

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.

Siponen, M., Mahmood, M.A., & Pahnila, S. (2014), Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.

Smith, W.K., & Lewis, M.W. (2011), Toward a Theory of Paradox: A Dynamic Equilibrium Model of Organizing. *Academy of Management Review*, 36, 381-403.

Steelman, Z.R., Lacity, M., & Sabherwal, R. (2016), Charting Your Organization's Bring-Your-Own-Device Voyage. *MIS Quarterly Executive*, (15)2, 85-104.

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. *MIS Quarterly*, *37*(4), 1141-1164.

Stutzman, F., Capra, R., & Thompson, J. (2011), Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27, 590-598.

Tu, Z., & Yuan, Y. (2015), Coping with BYOD Security Threat: From Management Perspective. *Twenty-first Americas Conference on Information Systems*, Puerto Rico.

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.

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), art. 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.

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.

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.

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.

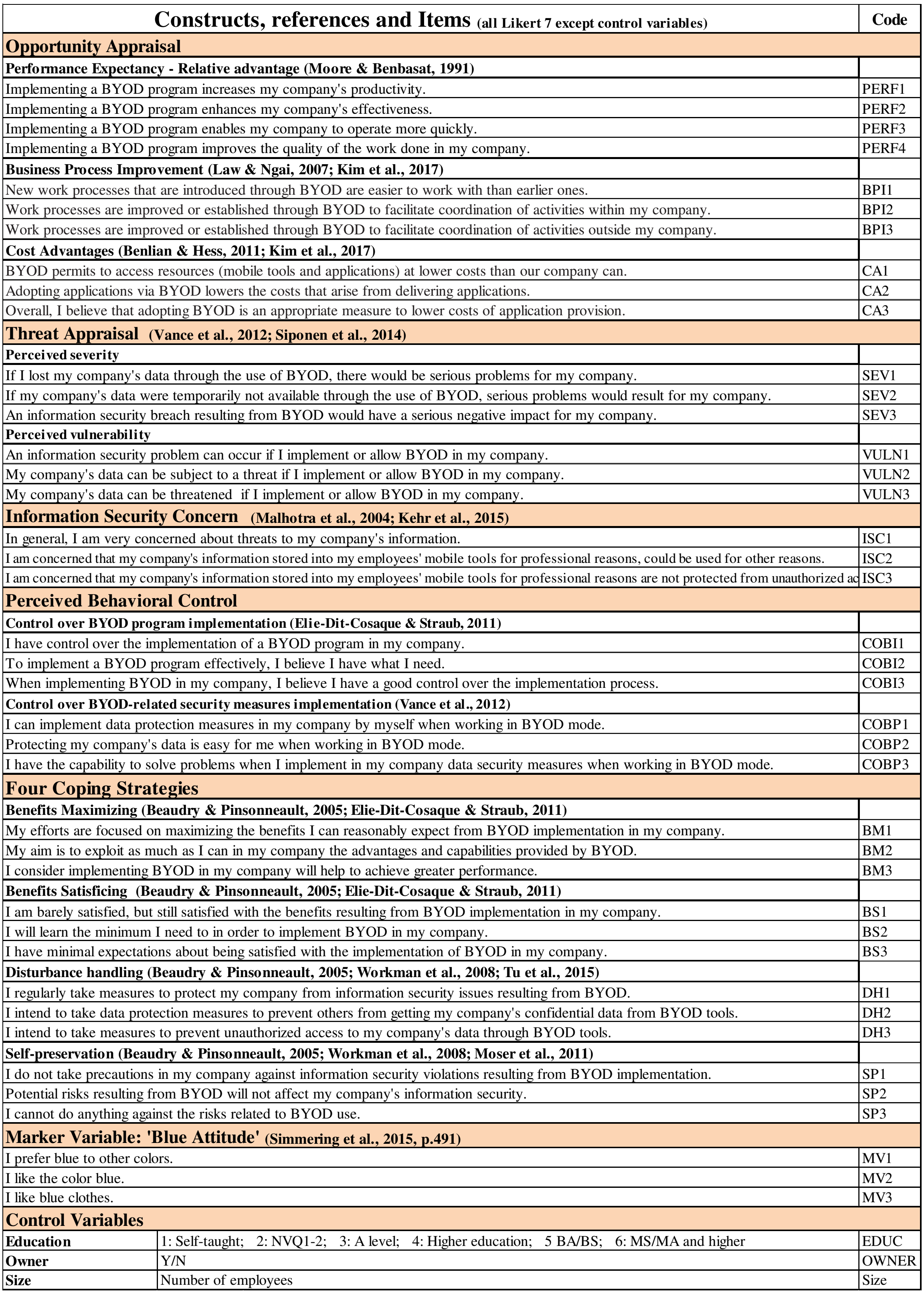
Weiss, F., & Leimeister, J.M. (2012), IT Innovations from the Consumer Market as a Challenge for Corporate IT. *Business & Information Systems Engineering* 6, 363-366.

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.

Zhou, T., Lu, Y. B., & Wang, B. (2010), Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, 26(4), 760-767.

Appendixes

Appendix A: Questionnaire and detailed constructs



Constructs, references and Items (all Likert 7 except control variables)		Code
Opportunity Appraisal		
Performance Expectancy - Relative advantage (Moore & Benbasat, 1991)		
Implementing a BYOD program increases my company's productivity.		PERF1
Implementing a BYOD program enhances my company's effectiveness.		PERF2
Implementing a BYOD program enables my company to operate more quickly.		PERF3
Implementing a BYOD program improves the quality of the work done in my company.		PERF4
Business Process Improvement (Law & Ngai, 2007; Kim et al., 2017)		
New work processes that are introduced through BYOD are easier to work with than earlier ones.		BPI1
Work processes are improved or established through BYOD to facilitate coordination of activities within my company.		BPI2
Work processes are improved or established through BYOD to facilitate coordination of activities outside my company.		BPI3
Cost Advantages (Benlian & Hess, 2011; Kim et al., 2017)		
BYOD permits to access resources (mobile tools and applications) at lower costs than our company can.		CA1
Adopting applications via BYOD lowers the costs that arise from delivering applications.		CA2
Overall, I believe that adopting BYOD is an appropriate measure to lower costs of application provision.		CA3
Threat Appraisal (Vance et al., 2012; Siponen et al., 2014)		
Perceived severity		
If I lost my company's data through the use of BYOD, there would be serious problems for my company.		SEV1
If my company's data were temporarily not available through the use of BYOD, serious problems would result for my company.		SEV2
An information security breach resulting from BYOD would have a serious negative impact for my company.		SEV3
Perceived vulnerability		
An information security problem can occur if I implement or allow BYOD in my company.		VULN1
My company's data can be subject to a threat if I implement or allow BYOD in my company.		VULN2
My company's data can be threatened if I implement or allow BYOD in my company.		VULN3
Information Security Concern (Malhotra et al., 2004; Kehr et al., 2015)		
In general, I am very concerned about threats to my company's information.		ISC1
I am concerned that my company's information stored into my employees' mobile tools for professional reasons, could be used for other reasons.		ISC2
I am concerned that my company's information stored into my employees' mobile tools for professional reasons are not protected from unauthorized ac		ISC3
Perceived Behavioral Control		
Control over BYOD program implementation (Elie-Dit-Cosaque & Straub, 2011)		
I have control over the implementation of a BYOD program in my company.		COBI1
To implement a BYOD program effectively, I believe I have what I need.		COBI2
When implementing BYOD in my company, I believe I have a good control over the implementation process.		COBI3
Control over BYOD-related security measures implementation (Vance et al., 2012)		
I can implement data protection measures in my company by myself when working in BYOD mode.		COBP1
Protecting my company's data is easy for me when working in BYOD mode.		COBP2
I have the capability to solve problems when I implement in my company data security measures when working in BYOD mode.		COBP3
Four Coping Strategies		
Benefits Maximizing (Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011)		
My efforts are focused on maximizing the benefits I can reasonably expect from BYOD implementation in my company.		BM1
My aim is to exploit as much as I can in my company the advantages and capabilities provided by BYOD.		BM2
I consider implementing BYOD in my company will help to achieve greater performance.		BM3
Benefits Satisficing (Beaudry & Pinsonneault, 2005; Elie-Dit-Cosaque & Straub, 2011)		
I am barely satisfied, but still satisfied with the benefits resulting from BYOD implementation in my company.		BS1
I will learn the minimum I need to in order to implement BYOD in my company.		BS2
I have minimal expectations about being satisfied with the implementation of BYOD in my company.		BS3
Disturbance handling (Beaudry & Pinsonneault, 2005; Workman et al., 2008; Tu et al., 2015)		
I regularly take measures to protect my company from information security issues resulting from BYOD.		DH1
I intend to take data protection measures to prevent others from getting my company's confidential data from BYOD tools.		DH2
I intend to take measures to prevent unauthorized access to my company's data through BYOD tools.		DH3
Self-preservation (Beaudry & Pinsonneault, 2005; Workman et al., 2008; Moser et al., 2011)		
I do not take precautions in my company against information security violations resulting from BYOD implementation.		SP1
Potential risks resulting from BYOD will not affect my company's information security.		SP2
I cannot do anything against the risks related to BYOD use.		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		
Education	1: Self-taught; 2: NVQ1-2; 3: A level; 4: Higher education; 5 BA/BS; 6: MS/MA and higher	EDUC
Owner	Y/N	OWNER
Size	Number of employees	Size

Appendix B: Measurement model

Table B1: Construct's internal consistency

	Composite Reliability	AVE	CTRL Implement	CTRL Protect	Sec Concern	Benef Max	Benef Sat	Disturb Handl	Self Preserv	Educ	Gender	Owner	Size
CTRL Implement	0.925	0.807	**0.898**										
CTRL Protect	0.914	0.779	0.695	**0.883**									
InfoSec Concern	0.838	0.721	-0.365	-0.394	**0.849**								
Benef Max	0.948	0.902	0.254	0.262	-0.241	**0.950**							
Benef Sat	0.742	0.594	0.027	0.106	-0.290	0.110	**0.771**						
Disturb Handl	0.912	0.776	-0.138	-0.140	0.495	-0.137	-0.099	**0.881**					
Self Preserv	0.875	0.699	0.198	0.169	-0.477	0.235	0.200	-0.623	**0.836**				
Educ	1.000	1.000	0.185	0.179	-0.013	0.093	-0.104	0.063	-0.070	**1.000**			
Gender	1.000	1.000	0.047	0.036	0.229	0.014	-0.081	0.053	-0.032	-0.213	**1.000**		
Owner	1.000	1.000	0.218	0.243	0.202	-0.116	-0.323	0.043	-0.163	-0.175	0.187	**1.000**	
Size	1.000	1.000	0.176	0.173	-0.060	-0.036	0.153	0.139	-0.221	0.081	0.034	-0.004	**1.000**

Squared root of the AVE in bold, along the diagonal.

Table B2: Discriminant Validity (HTMT)

	Benef Max	Benef Sat	CTRL Implem ent	CTRL Protect	Disturb Handl	Educ	Gender	Opport	Owner	Sec Concern	Self Preserv	Size	Threat
Benef Max													
Benef Sat	0.298												
CTRL Implement	0.279	0.235											
CTRL Protect	0.358	0.217	0.720										
Disturb Handl	0.248	0.136	0.234	0.232									
Educ	0.120	0.075	0.228	0.227	0.043								
Gender	0.110	0.282	0.059	0.117	0.054	0.255							
Opport	0.613	0.606	0.333	0.225	0.222	0.155	0.205						
Owner	0.166	0.153	0.187	0.139	0.053	0.242	0.153	0.203					
Sec Concern	0.458	0.443	0.441	0.625	0.699	0.108	0.301	0.287	0.036				
Self Preserv	0.380	0.243	0.174	0.200	0.715	0.052	0.059	0.317	0.210	0.626			
Size	0.111	0.227	0.239	0.237	0.183	0.102	0.042	0.174	0.003	0.316	0.303		
Threat	0.535	0.408	0.344	0.493	0.733	0.093	0.242	0.470	0.114	0.890	0.724	0.209	

Tables B3: Validity of the second order constructs

First order constructs' internal consistency

	Composite Reliability	Average Variance Extracted
Biz Process	0.848	0.650
Cost Adv	0.936	0.830
Perf Expect	0.926	0.759
Severity	0.855	0.747
Vulnerability	0.948	0.901

Composite reliability is > 0.7 and AVE are > 0.5.

Variance Inflation factors VIF

	Opport	Threat
Biz Process	1.607	
Cost Adv	1.238	
Perf Expect	1.504	
Severity		1.602
Vulnerability		1.602

All VIF are < 5: potential collinearity between the constructs forming the second order constructs is not a critical issue in this model (Hair et al., 2018, p.62).

Path coefficient and significance of First order constructs on second order constructs.

Variable Influence	Beta	T Statistics	P Values
Performance Expectancy -> Opport	0.550	9.920	0.000
Cost Advantage -> Opport	0.390	6.845	0.000
Biz Process Improvement -> Opport	0.314	7.477	0.000
Perceived Severity -> Threat	0.502	13.796	0.000
Perceived Vulnerability -> Threat	0.610	16.631	0.000

Path coefficient are relatively balanced and exhibit strongly significant P-values.