Information security in SMEs: determinants of CEOs' protective and supportive behaviors

Yves BARLETTE & Annabelle JAOUEN

Montpellier Business School, France

ABSTRACT

This research addresses the determinants of CEOs' actions regarding the information security (ISS) of small and medium enterprises (SMEs). This article aims to (a) identify factors influencing CEOs' ISS actions, (b) examine the relevance of protection motivation theory (PMT) in explaining top management support (TMS, i.e., supportive actions), and (c) find potential differentiated effects on protective vs. supportive actions.

The results of a questionnaire-based survey (N=200) show that the PMT and social influence constructs, while explaining a significant amount of variance, exert differentiated effects: in contrast with protective actions, which are influenced mainly by self-efficacy, SME CEOs' supportive actions are strongly affected by the social influence of peers (partners and competitors) and customers.

At a theoretical level, this research validates the relevance of the PMT framework for the study of TMS determinants in the context of ISS. This study is also the first to distinguish between these two types of actions and offers new insights on CEOs' ISS-related behavior literature. For practitioners, the results imply that even when CEOs do not exert protective actions, it is important to build on their professional relations to trigger and enhance their supportive actions.

Keywords: *ISS, CEO, SME, Protection motivation theory, Top management support.*

RÉSUMÉ

Cette recherche porte sur les déterminants des comportements en sécurité de l'information (SSI) des dirigeants de PME, en distinguant les actions de protection des actions de soutien. Cet article vise à (a) identifier certains des facteurs qui influencent leurs comportements en SSI, (b) examiner la pertinence de la Protection Motivation Theory (PMT) pour expliquer le Top Management Support (TMS, c.-à-d. le soutien du dirigeant) et (c) mettre en évidence d'éventuels effets différenciés selon les actions de protection et de soutien.

Les résultats, provenant d'une étude quantitative (N=200), montrent que les construits de la PMT et l'influence sociale expliquent une part significative de la variance, mais exercent

également des effets différenciés : alors que les actions de protection sont prioritairement influencées par l'auto-efficacité, les actions de soutien des dirigeants sont essentiellement affectées par l'influence sociale des pairs (partenaires et concurrents) et des clients.

Au niveau théorique, cette recherche établit la pertinence de la PMT pour étudier les déterminants du TMS dans le contexte de la SSI. Cette étude est également la première qui distingue ces deux types d'actions et offre ainsi de nouveaux éléments de compréhension des comportements des dirigeants de PME en SSI. Pour les praticiens, nos résultats mettent en évidence que même si les dirigeants n'agissent pas directement, il est important de prendre en considération l'entourage professionnel du dirigeant de PME de manière à développer ses actions de soutien.

Mots-clés : *Sécurité de l'information, Dirigeant, PME, Protection motivation theory, Top management support.*

1. INTRODUCTION

Small and medium enterprises (SMEs, i.e., firms with fewer than 250 employees) constitute more than 99% of European firms (European Union, 2016) and are more vulnerable to threats than large companies because they do not often place adequate weight on information security (ISS) (Ismail, 2018). One in three SMEs had no safeguards to prevent breaches, and 61% of data breach victims in 2017 were SMEs (Ismail, 2018). Security breaches not only endanger SMEs but also allow access to larger firms through the Internet or exchanges between partners, dramatically increasing these large firms' vulnerability to cyber-attacks (Lábodi & Michelberger, 2010; Nice, 2018).

Top managers have a very important role to play, as they are usually the decision makers regarding ISS (Hu *et al.*, 2012; Puhakainen & Siponen, 2010). In the SME context, top management often includes the CEO (Curran & Burrows, 2015). Hence, CEOs can decide or validate the implementation of ISS-related measures; they can also provide resources, such as funding, act as change agents to establish a more secure company culture or, if necessary, enforce employee compliance with ISS measures (Knapp *et al.*, 2006). Raising CEOs' awareness about the need to implement ISS measures is therefore critical for SMEs and, by extension, for large firms. A second reason for studying SME CEOs is that they exhibit specific decision-making processes that differ from those of the CEOs of large companies (Jaouen & Nakara, 2015; Kyobe, 2008). Hence, focusing on SMEs' ISS-related decisions may provide new knowledge on the specificities of SME CEOs.

Previous ISS research has focused mainly on employee compliance with ISS policies (Karjalainen *et al.*, 2019; Moody *et al.*, 2018; Yazdanmehr & Wang, 2016). It has also addressed executives and employees, notably comparing information technology (IT) and non-IT specialists. Previous studies

have investigated either behavioral intention (e.g., Moody *et al.*, 2018), actual behavior (e.g., Chen & Zahedi, 2016), or both (e.g., Mwagwabi *et al.*, 2018). However, in terms of actors, the ISS literature has rarely focused on SME CEOs, except a few studies on cyber security and CEO behavior (Berry & Berry, 2018; Fielder *et al.*, 2016) or on the need to develop an ISS culture (Barlette *et al.*, 2017; Dojkovski *et al.*, 2007).

In terms of behaviors, in contrast with employees, SME CEOs can exert two types of actions. They can take *protective actions* by implementing security measures, for example, but even if they lack the necessary skills to implement them personally, CEOs may be conscious of security issues and act less "directly" by providing support to ISS projects through funding (Boonstra, 2013; Lin *et al.*, 2014), supporting the persons in charge (e.g., the IT specialist or the chief information officer when (s)he exists) or championing and raising employee awareness (Boonstra, 2013; Chen *et al.*, 2012). In this paper, we assimilate these *supportive actions* into what is called top management support (TMS).

While the impacts of CEOs on the success of IS and ISS projects have been the subject of extensive research (e.g., Hu *et al.*, 2012; Lee *et al.*, 2018), academic attention to the determinants of TMS regarding IS is still emerging in the literature. Studies have focused mainly on the influence of demographic variables, such as gender, age, and education (Lin *et al.*, 2014; López-Muñoz & Escribá-Esteve, 2017), or on how IT managers could obtain TMS (Liu *et al.*, 2015). Regarding ISS, behavioral research integrated threat appraisal as a particularly influencing dimension. For instance, it appeared as a building block in the Technology Threat Avoidance Theory (TTAT, Liang & Xue, 2010), the Health Belief Model (HBM, Ng *et al*., 2009) and the Protection Motivation Theory (PMT, Rogers, 1983). Therefore, we can assume that in contrast to IS, the determinants of ISS-related behaviors, either protective or supportive (TMS), are particularly influenced by threat appraisal. Moreover, to our knowledge, only one qualitative study on the determinants of the involvement of CEOs regarding ISS can be identified (Barlette, 2012). Considering the scarcity of relevant academic research and the importance of this issue, the first gap we intend to fill is the identification of factors influencing SME CEOs' ISS-related protective and supportive behaviors.

For this purpose, we used protection motivation theory (PMT). PMT is one of the main reference theories used to explain security-related behaviors (Williams *et al.*, 2014). While this theory's explanatory power for protective actions has been repeatedly shown, the second gap we intend to fill is to validate the relevance of the PMT constructs in explaining TMS, i.e., CEOs' supportive actions.

In the specific case of SME CEOs, several recent surveys have also proven the impact of social influence on security behaviors (Barlette *et al.*, 2017; Tsai *et al.*, 2016). Through a comparison of the effects of the PMT constructs and social influence on CEOs' protective and supportive actions, this paper aims to highlight discrepancies between the impacts of the various determinants of ISS-related behaviors. Hence, through the use of PMT and TMS as theoretical foundations, the third gap we intend to fill concerns highlighting the potentially differentiated effects of the PMT and social influence constructs on protective and supportive actions.

The model, tested on 200 SME CEOs, indicates that the determinants exert a differentiated influence according to the type of action. Self-efficacy has the most explanatory power for protective actions, whereas social influence is the main driver of supportive actions. These findings offer a

new perspective to better understand CEOs' ISS-related actions using latent endogenous constructs that have not been previously distinguished in IS research, that is, protective and supportive actions. The findings are expected to inform theory and practice in this under-researched area.

This article is structured as follows. In the next section, relevant literature is reviewed, and a theoretical background is developed. In the third section, hypotheses are developed, and the research model is presented. Then, the research method is described, analytical procedures are outlined, and the results are presented. These results are discussed in section six, where we present our contributions to theory and practice, the study's limitations and avenues for future research.

2. THEORETICAL BACKGROUND

ISS is not only a matter of IT security, anti-malware programs, firewalls, efficient identification systems or reliable hardware (Williams *et al.*, 2014); it is also an organizational, cultural and managerial issue (Abubakare *et al.*, 2017). ISS is often threatened by employee behavior that does not comply with ISS policies (Chu & Chau, 2014), organizational rules, guidelines or requirements (Workman *et al.*, 2008) and by the negligent handling or purposeful damage of information by internal employees or strategic partners (i.e., suppliers, partners, and customers) with access to company databases (Lábodi & Michelberger, 2010).

Friend & Pagliari (2000) confirmed the important role of top management in ISS: "*in any organization, top management has ultimate responsibility for security. Any action taken, or problem solved should be a result of top management's intervention*" (p. 31). Top management, specifically the CEO in the case of SMEs, can significantly reduce risk and ensure employee ISS compliance by implementing ISS policies and procedures. However, the CEO can also support the person in charge of ISS (chief information officers (CIOs), when the position exists, or internal or external IT specialists). TMS, i.e., supportive actions, has been shown to affect organizational culture and employees' salient beliefs regarding ISS policies and procedures (Hu *et al.*, 2012; Pérès *et al.*, 2003; Puhakainen & Siponen, 2010). Because of SME CEOs' specificities, investigating both types of actions seems particularly relevant in this context.

2.1. SME CEOs' protective actions

CEOs and top management actions in ISS are essential to reducing risk and ensuring employee ISS compliance (de Guinea *et al.*, 2005; Hu *et al.*, 2012). Through their actions, CEOs can enforce the necessary rules and processes for ISS management and provide the basis of a coherent ISS approach. CEO actions improve the legitimacy of ISS measures, influence employees and act as change agents to create a favorable environment to overcome organizational resistance (Kankanhalli *et al.*, 2003; Knapp *et al.*, 2006). Therefore, CEOs' actions in ISS are highly desirable in businesses of every size (Rainer *et al.*, 2007).

CEOs develop protective actions when they personally take basic technical ISS measures (changing passwords, performing backups, etc.) (Lee & Larsen, 2009). Other examples of top management protective actions include implementing new security procedures or contacting external support to repair employee computer damage, solving basic security problems or managing relations with external providers (Barlette, 2012).

In small businesses, CEOs are the main (and often the sole) decision makers and strategic information users. They are therefore in the best position to identify critical business applications to computerize or protect (Kankanhalli *et al.*, 2003). The IS literature shows that SME CEOs develop specific decision-making processes that differ from those of the CEOs of large companies (Nguyen *et al.*, 2015; Senyard *et al.*, 2011). Scholars have been particularly interested in how the SME context of high uncertainty, time pressure, emotional intensity, and/or high risk affects decision-making (Mullins & Forlani, 2005; Shepherd *et al.*, 2015). For instance, Mitchell & Shepherd (2010) showed that decisions in SMEs are particularly influenced by CEOs' fear of failure and level of self-efficacy. Moreover, SME CEOs have difficulties delegating, tend to act and decide alone, and tend to take organizational measures by themselves (Curran & Burrows, 2015; Torres & Julien, 2005).

Consequently, SMEs lag behind larger firms in implementing protective measures because in this context, decision-making is strongly related to a CEO's ability to process and exploit the available information (Lábodi & Michelberger, 2010; Rainer *et al.*, 2007). These limitations are both cognitive and technical (i.e., constraints in accessing and using information). First, SME CEOs lack technical and financial resources (Lábodi & Michelberger, 2010; Lee & Larsen, 2009), and second, they are not sufficiently qualified to correctly handle technologies and security issues (Kyobe, 2008). Therefore (a) it is difficult for SMEs to recruit and keep IT specialists (Pritchard, 2010); (b) ongoing risk assessment is often lacking (Nguyen *et al.*, 2015); (c) many SME CEOs are not sufficiently aware of ISS issues (Barlette *et al.*, 2017); and (d) many of these CEOs consider ISS to be a large business concern (Nice, 2018). Because their ISS is poorly aligned with strategy, SMEs may implement inadequate hardware and software, and information may be poorly secured. Many CEOs rely on external human resources for IT implementation and support (Rainer *et al.*, 2007). Others neglect ISS management even if, paradoxically, they positively perceive the importance of ISS in their firms (Rainer *et al.*, 2007). External influences, through their personal and professional networks, may trigger their decisions to undertake protective actions (Barlette & Jaouen, 2012). Thus, CEOs can decide to surround themselves with internal or external staff skilled in ISS and then exert supportive actions.

2.2. Top management support

2.2.1. TMS and types of supportive behaviors

TMS is an umbrella term that includes several notions, such as involvement and participation (Kulkarni *et al.*, 2017). TMS usually relies on supportive attitudes and behaviors that can be categorized into three main types, i.e., involvement, participation and resource provision (Liu *et al.*, 2015).

Involvement corresponds to the top management's psychological state, that is, CEOs' perceptions and attitudes, reflecting the degree of importance placed on IT (Jarvenpaa & Ives, 1991) and, in our context, on ISS. Top management involvement and commitment must be demonstrated through CEOs' sincere and effortful participation (Liu *et al.*, 2015), which is critical to project success (Dong *et al.*, 2009).

Participation refers to "*the CEOs' activities or substantive personal interventions in the management of IS*" (Jarvenpaa & Ives, 1991, p. 206). Participation translates into important manifestations of TMS through presence and visibility. Hence, top management can directly influence

the mutual adaptation between the IS project and the organization (Kulkarni *et al.*, 2017). For example, top managers can help solve management problems and adapt inadequate organizational structures or processes. CEO participation can also translate into *project championing* (Lin *et al.*, 2014; McComb *et al.*, 2008), which refers to "*very clearly communicating the crucial importance of the project, resolving conflicts, and unequivocally supporting the project team*" (Boonstra, 2013, p. 500). Dong *et al.* (2009) also identified change management and *vision sharing* as distinct types of TMS-related behaviors. In the same vein, Gottschalk (1999) measured TMS in terms of 'enthusiasm and IT vision'. Hence, participation can be associated with a clear vision (Liang *et al.*, 2007), which can be shared with employees through project championing.

Resource provision is the third[1] and widely acknowledged supportive aspect of top management (Boonstra, 2013). It corresponds to allocating funds, validating budgets, assigning personnel and equipment to an IT project, and building an enabling context that facilitates the flow of resources (Liu *et al.*, 2015).

2.2.2. Effects of TMS in IS and ISS

A rich body of literature has been developed to theorize the impact of TMS on the success of IS development, adoption, implementation, and assimilation (Elbanna, 2013; Shao *et al.*, 2016; Staehr, 2010) and has highlighted the essential role of TMS in the success of IS projects (Dong *et al.*, 2009; Elbanna, 2013; Lee *et al.*, 2018; Liu *et al.*, 2015). Shao *et al.* (2016, 2017) showed that a combination of transformational and transactional leadership skills is necessary for adequate TMS in IS projects. Kulkarni *et al.* (2017) showed that top management championship leads to higher employee participation and encourages employee engagement as meaningful contributors to technology advancements. Therefore, employees actively participate "*in continually improving the systems they routinely use via submitting feedback and suggestions, critically evaluating the functionalities, asking for enhancements, trying out new features, and, in general, being responsible for their success*" (Kulkarni *et al.*, 2017, p. 534). In the ISS context, previous research has shown that TMS is essential (Puhakainen & Siponen, 2010) and that top management should be actively and visibly involved in the establishment, implementation, and enforcement of ISS policies and rules (Hu *et al.*, 2012). Top managers can help increase individual employees' awareness of ISS policies and foster a common favorable disposition toward compliance and ethical behaviors (Boss *et al.*, 2009; Chen *et al.*, 2012; Li *et al.*, 2010).

However, top management executives usually do not possess core expertise in ISS, and they often delegate the authority and responsibility to establish and maintain ISS policies to IT specialists (CIOs) or ISS experts, such as CISOs[2] (Merhi & Ahluwalia, 2015). In addition, in the smallest SMEs, there are often no CIOs, and even in the largest SMEs, experts in ISS remain scarce. Another delegation is possible: the CEO can outsource to external actors, such as IT specialists or IT service companies. However, in all cases, addressing ISS issues cannot be a full-time job for CIOs or internal or outsourced IT specialists. Rothrock *et al.* (2018) advocated that top managers must understand the issues at stake and accept their responsibility for their organization's

[1] Some authors consider resource provision as a component of participation because it refers more to behaviors than to attitudes (Dong *et al.*, 2009).

[2] Chief information security officer.

cyber defense posture. However, Elbanna (2013) showed that TMS fluctuates during the course of any project from moments of direct involvement to moments of low attention and enthusiasm. Hence, in the case of multiple projects, priorities for projects can change and, in turn, top management attention and resource allocation can be redirected toward other projects (Kappelman *et al.*, 2006). This fluctuation can even lead to withholding TMS because support is a scarce resource in terms of finances, power, people, communication, attention, expertise, and time (Boonstra, 2013). Hence, because "*Top managers are often pressurized into choosing between current organizational activities and new initiatives*" (Boonstra, 2013, p. 510), management support can be limited by competing projects, project risks, and business priorities.

Given the importance of ISS and the need to maintain ISS issues among the top management priorities, more research should be conducted on the factors that influence TMS in ISS (Liu *et al.*, 2015) and the identification of these determinants of TMS (Lin *et al.*, 2014; Štemberger *et al.*, 2011).

2.2.3. Antecedents of top management support

While the impacts of TMS have been explored in numerous studies, the antecedents of TMS in IS projects remain under-researched (see table 1). Most previous studies have addressed the CEOs' or CIOs' demographic indicators and characteristics, mainly in terms of age, education, openness to experience and IT experience (Lin *et al.*, 2014; López-Muñoz & Escribá-Esteve, 2017). Only three studies have explored additional behavioral factors. Štemberger *et al.* (2011) investigated how IT/IS personnel can obtain support from top management and found that the business and managerial knowledge and skills of IT/IS personnel and the business role of IT/IS had a positive impact on achieving TMS. Liu *et al.* (2015) showed that IT teams can obtain TMS by appropriately building and mobilizing social capital, i.e., socializing, interacting and building ties with top management. López-Muñoz & Escribá-Esteve (2017) added two processes to the demographic indicators cited above: participatory decision-making and shared IT vision.

Impact of TMS		**Determinants of TMS**	
IS projects	**ISS**	**IS projects**	**ISS**
Elbanna (2013)	Puhakainen & Siponen (2010)	Štemberger *et al.* (2011)	Barlette (2012)
Kanwal *et al.* (2017)	Chen *et al.* (2012)	Lin *et al.* (2014)	(qualitative)
Kulkarni *et al.* (2017)	Hu *et al.* (2012)	Liu *et al.* (2015)	
Shao *et al.* (2016)	Kwon *et al.* (2013)	López-Muñoz & Escribá-Esteve (2017)	
Shao *et al.* (2017)	Merhi & Ahluwalia (2015)		
Lee *et al.* (2018)	Zafar *et al.* (2016)		
	Daud *et al.* (2018)		
	Rothrock *et al.* (2018)		

Table 1: Recent studies[3] on the *impacts* and the *determinants* of TMS.

[3] For conciseness, we included only studies from 2010 on TMS effects.

In the context of ISS, to the best of our knowledge, quantitative research has never been used to explore the determinants of supportive actions (see table 1). However, we have shown that CEOs' supportive actions have significant impacts on firm security, and consequently, exploring the factors triggering supportive actions in ISS is particularly relevant.

The protection motivation theory (PMT) is regularly used to study ISS-related actions (see Appendix A). In addition to its power to explain ISS protective actions, we postulate that this theory is also relevant for analyzing the determinants of ISS supportive actions.

2.3. Determinants of SME CEOs' ISS behaviors

2.3.1. Protection motivation theory

Previous ISS research aiming to explain security-related behavior has mainly adopted the PMT as the reference theory (Williams *et al.*, 2014). The output of the PMT model "*is the decision (or intention) to initiate, continue, or inhibit the applicable adaptive responses (or coping behaviors)*" (Floyd *et al.*, 2000, p. 411). Even if PMT "*hypothesized that protection motivation is best measured by behavioral intentions*" (Rogers, 1983, p. 172), this theory "*is sufficiently broad to apply to any situation involving threat*" (Rogers, 1983, p. 172), i.e., single-act, repeated-acts, or multiple-acts behavioral criteria (Prentice-Dunn & Rogers, 1986). Consequently, depending on the type of behavior investigated, several streams of PMT-based research have explored — in a relatively balanced manner (see Appendix A) — either behavioral intention (Moody *et al.*, 2018; Tsai *et al.*, 2016; Tu *et al.*, 2015), actual behavior (Chen & Zahedi, 2016; Posey *et al.*, 2015) or both (Thompson *et al.*, 2017; Warkentin *et al.*, 2016).

Empirical research on PMT focuses on the relationship between potential threat and coping mechanisms and outcomes (Crossler & Bélanger, 2014). Two processes determine an individual's motivation to protect information (Maddux & Rogers, 1983): threat appraisal and coping appraisal. Threat appraisal is the individual's anticipation of a psychological, sociological or physical violation or harm to oneself (Workman *et al.*, 2008). When the perceived vulnerability and severity of this threat are high, an individual modifies his or her behavior and is more likely to exert an adaptive response.

Coping appraisal relates to an individual's evaluation of his or her ability to cope with and avoid threatening behavior. Three components influence this evaluation: the individual's response efficacy, that is, the perceived effectiveness of the proposed adaptive behavior, the individual's self-efficacy, i.e., the perceived ability to perform the adaptive behavior, and the individual's response cost, i.e., the inconvenience, money or time related to the adaptive behavior. We chose not to include response cost in this study because it is the most questionable construct in terms of applying PMT to ISS. In 29 previous studies (see Appendix A), the expected effect was proven only 9 times. This construct was not valid 9 times when included (e.g., Crossler & Bélanger, 2014; Ifinedo, 2012; Mwagwabi *et al.*, 2018; Siponen *et al.*, 2014) and was not included 11 times (e.g., Chen & Zahedi, 2016; Johnston *et al.*, 2015; Moody *et al.*, 2018; Warkentin *et al.*, 2016).

Furthermore, several studies integrated the social influence construct into the core PMT model. This construct has been added 13 times in previous studies (see Appendix A) and proved to be significant in 69 percent of the cases. Indeed, research on small businesses has shown that CEOs often rely on their social and professional networks to make decisions and that such social

influences may constitute a relevant variable to explain CEO behaviors (Barlette *et al.*, 2017; Ozgen & Baron, 2007; Schoonjans *et al.*, 2013).

2.3.2. The role of social influence

Social influence is a multifaceted construct that closely resembles social norms (Johnston & Warkentin, 2010; Venkatesh *et al.*, 2003), subjective norms (Ifinedo, 2012; Yazdanmehr & Wang, 2016) and normative beliefs (Siponen *et al.*, 2014). In this study, we consider social influence to be "*the perception of a person that most people important to him/her think he/she should or should not perform the behavior in question*" (Fishbein & Ajzen, 1975, p. 302). Social influence research focuses on how social networks influence behavior through messages and signals that intend to build or change perceptions of an activity's value (Herath & Rao, 2009; Tsai *et al.*, 2016).

Among the different approaches to social influence, Bandura's (1977, 1986) social learning theory has been viewed as particularly influential (Tu *et al.*, 2015). He explained that human behavior is stimulated first by external influences, then by internal processing systems and regulatory codes, and finally by the reinforcement of response-feedback systems. Self-observations and feedback from the social environment are the basis upon which situational assessments (judgments) are developed, which, in turn, drive intentions for adjusting behaviors (Tu *et al.*, 2015). Consequently, individuals are influenced by both messages about expectations and the observed behavior of others (Herath & Rao, 2009). Johnston & Warkentin (2010) noticed that influences from family, friends, colleagues, or trusted others within the organization are highly important in IT decisions. Contractor & Eisenberg (1990) discussed "social contagion" and distinguished two network models of contagion. First, the relational model focuses on the influence of people with whom an individual has direct interactions. Second, the positional model, also called the structural equivalence model (Burkhardt, 1994; Burt, 1987), shows that people are influenced by those with whom they have the same patterns of communication, even though they may not interact directly (e.g., people with the same position within an organization). Burkhardt (1994) also showed that social interactions with one category or another differentially affect the frequency with which individuals use IT, their attitude toward IT, and their sense of self-efficacy regarding IT. Perceptions about others' opinions may also predict attitudes toward security-related behaviors (Anderson & Agarwal, 2010; Tsai *et al.*, 2016).

Lewis *et al.* (2003) stated that *"if a peer, supervisor, or some other actor in a relevant social network believes that a technology is useful, through a process of shared cognition, so will the target individual"* (p. 662). By definition, because CEOs do not have supervisors, peers or actors in their social network can encourage them to take IS or ISS measures (Barlette *et al.*, 2017). CEOs may, for example, be verbally persuaded by peers to take recommended actions (Tu *et al.*, 2015). However, this influence can also have an effect indirectly through the observed actions of peers, mentors or competitors (Dagorn & Poussing, 2012; Ozgen & Baron, 2007; Tu *et al.*, 2015; Zhang *et al.*, 2018).

2.4. Protective vs. supportive behaviors

Barlette (2012) conducted a qualitative study in which he showed that SME CEOs can adopt four types of behaviors (Figure 1). When they are poorly involved, they do not tend to exert protective actions, except reactive actions when it is absolutely necessary (case 'A', e.g., failure or security

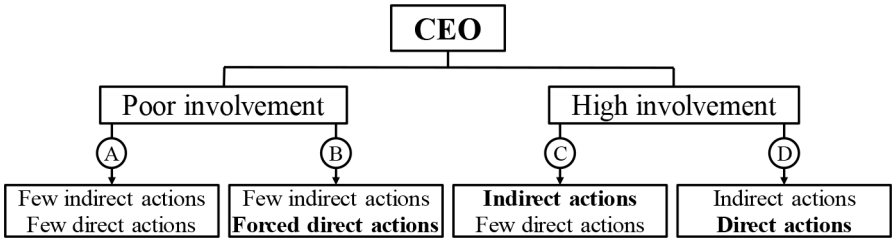

Figure 1: Coexistence of both types of behaviors, adapted from Barlette (2012).

breach) or compulsory (case 'B', e.g., regulations). Moreover, even if someone else takes charge of the company's ISS, CEO's support will be weak.

According to Barlette (2012), when CEOs' involvement increases, they tend to interact more with and provide more support to the persons in charge of ISS, either the internal CIO if he/she exists or an external provider (cases 'C' and 'D'). Through these interactions, CEOs learn more about IS and ISS and become familiar with ISS issues, therefore improving their awareness. Consequently, some CEOs feel more comfortable with ISS or learn on-the-job and tend to exert more protective actions (case 'D'). The level of supportive and mainly protective actions will depend on the CEOs' priorities, i.e., the balance between business situations and security issues. This figure shows that both types of behaviors (protective and supportive) can coexist. However, if he identified several determinants of CEO involvement, Barlette (2012) conducted a qualitative study that needs to be generalized.

3. CONCEPTUAL MODEL AND HYPOTHESIS DEVELOPMENT

In our theoretical background, we noted that distinguishing between protective and supportive actions is relevant to the specific context of SME CEOs. Consequently, we investigate both types of actions (see Figure 2). First, we study the usual measures of protective actions, i.e., implementing ISS measures and performing "technical behaviors", such as antivirus updates or backups (Lai *et al.*, 2012). Second, we also consider supportive actions, that is, validating IS security measures or budgets, supporting the person in charge of ISS or raising employees' awareness.

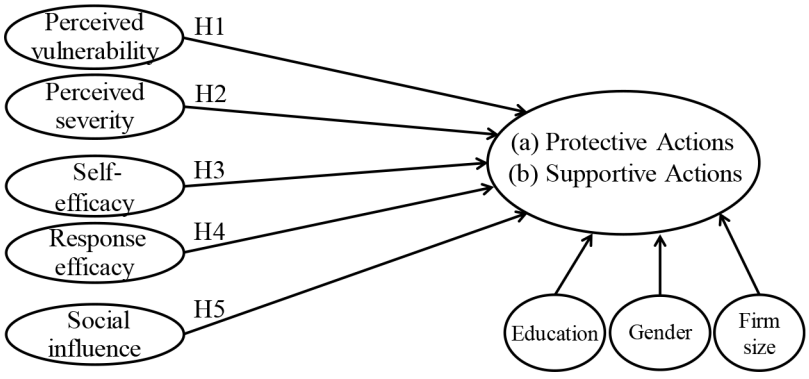

Figure 2: Research model.

The conceptual model aims to explain CEOs' actual behaviors, not their intentions. Measuring actual behavior prevents research from reaching incorrect conclusions (Limayem *et al.*, 2007) because it is more objective than intention and because self-reported behavior is often easier to self-assess (Ng *et al.*, 2009). Moreover, we investigate behaviors that can be repetitive, and in that case, intentions no longer matter (Crossler & Bélanger, 2014).

The hypotheses indicate that protective and supportive actions are a positive linear function of five constructs: perceived vulnerability to the threat, perceived severity of the threat, self-efficacy, response efficacy, and social influence. Because their level of impact may vary according to the type of action, we present a differentiated set of hypotheses for protective and supportive actions.

3.1. Perceived vulnerability

Perceived vulnerability is an individual's belief about "*the conditional probability that the threatening event will occur, provided that no adaptive activity is performed*" (Rogers, 1983, p. 158). The results concerning this construct in previous literature are contradictory. While several studies reveal a positive influence of perceived vulnerability on ISS-related protective actions (e.g., Chen & Zahedi, 2016; Ng *et al.*, 2009; Workman *et al.*, 2008), others find no significant effect (e.g., Herath & Rao, 2009; Vance *et al.*, 2012). Johnston *et al.* (2015) explained these contradictory findings, arguing that threat appraisal constructs are not personally relevant for employees in an organizational context because they have a lesser sense of ownership and interest in their firm's data. We suppose that for SME CEOs, perceived vulnerability remains a relevant construct to explain protective actions because SME CEOs tend to identify themselves much more strongly with their firms than their employees do (Jaouen & Lasch, 2015). Hence, as the perceived vulnerability to a security breach increases, SME CEOs will display more ISS behaviors. Therefore, the following hypothesis is proposed:

H1a: Perceived vulnerability positively influences SME CEOs' protective actions in their companies.

To the best of our knowledge, no previous studies have addressed the determinants of TMS (supportive actions) in ISS. We can assume that CEOs' protective and supportive actions are similarly influenced by perceived vulnerability and that this construct will exert a similar effect on both types of actions. Therefore, we formulate the following hypothesis:

H1b: Perceived vulnerability (1) positively influences SME CEOs' supportive actions in their companies, and (2) this influence will be similar to that on protective actions.

3.2. Perceived severity

Perceived severity corresponds to an individual's perception of the severity of the consequences of a threat (Maddux & Rogers, 1983). For instance, threats may include the perceived level of the company's financial losses, the decrease in activity, the loss of data, and/or the indirect damage to the company's image. Most previous studies reveal that an increase in perceived severity exerts a significant effect on an individual's ISS-related behavior (Chen & Zahedi, 2016; Crossler & Bélanger, 2014). However, as for perceived vulnerability, some studies find contradictory results when addressing employees' behaviors (Ifinedo, 2012; Johnston *et al.*, 2015; Ng *et al.*, 2009). Following the same reasoning as that for perceived vulnerability, in the context of SME CEOs, the following hypothesis is therefore proposed:

H2a: Perceived severity positively influences SME CEOs' protective actions in their companies.

As for H1, we assume that perceived severity will exert the same effect on supportive actions due to the lack of prior research; hence, we posit the following:

H2b: Perceived severity (1) positively influences SME CEOs' supportive actions in their companies, and (2) this influence will be similar to that on protective actions.

3.3. Self-efficacy

Self-efficacy refers to individuals' belief that they can successfully implement a protective behavior (Vance *et al.*, 2012). Prior ISS research has demonstrated a significant influence of self-efficacy on the motivation to exert protective behaviors in many contexts (Chen & Zahedi, 2016; Crossler & Bélanger, 2014; Lee & Larsen, 2009; Workman *et al.*, 2008). In our context, self-efficacy refers to CEOs' beliefs in their own abilities to *personally* implement ISS measures and perform antivirus updates and backups. Several PMT studies focusing on protective actions have shown that self-efficacy has a highly strong influence (usually b>=0.5) on such actions (Chen & Zahedi, 2016; Crossler & Bélanger, 2014; Gurung *et al.*, 2009; Hanus & Wu, 2016; Li *et al.*, 2019). On the other hand, Lee & Larsen (2009) showed that self-efficacy exerted the weakest influence of the PMT constructs on one dimension of supportive actions, that is, the intention to validate the budget of an ISS measure. Consequently, we can suppose that because protective actions are more technical (Lai *et al.*, 2012) than providing TMS, i.e., exerting supportive actions, the effect of their perceived self-efficacy will be higher on protective actions than on supportive actions. Therefore, the following hypotheses are proposed:

H3a: Perceived self-efficacy positively influences SME CEOs' protective actions in their companies.

H3b: Perceived self-efficacy (1) positively influences SME CEOs' supportive actions in their companies, and (2) this influence will be lower than that on protective actions.

3.4. Response efficacy

Response efficacy corresponds to individuals' belief that protective behavior will result in effective protection against IS security threats (Vance *et al.*, 2012). In our context, response efficacy refers to CEOs' beliefs about whether exerting protective (e.g., implementing ISS-related measures) or supportive actions can enhance their companies' security and reduce security breaches. Previous ISS work has demonstrated that response efficacy exerts a significant positive effect on protective behaviors (Chen & Zahedi, 2016; Crossler & Bélanger, 2014; Workman *et al.*, 2008). Therefore, the following hypothesis is proposed:

H4a: Perceived response efficacy positively influences SME CEOs' protective actions in their companies.

We found no hint in the literature about a differentiated influence of perceived response efficacy on protective and supportive behaviors. We can assume that this influence will be the same for both types of behaviors: for example, the motivation to validate the implementation or to conduct awareness raising will be the same as implementing an ISS measure if the response is perceived as efficient. Therefore, we formulate the following hypothesis:

H4b: Perceived response efficacy (1) positively influences SME CEOs' supportive actions in their companies, and (2) this influence will be similar to that on protective actions.

3.5. Social influence

Social influence has been incorporated into the PMT model in several studies and has been found to be a significant predictor of computer security-related policy or software adoption (Herath & Rao, 2009; Ifinedo, 2012; Lee & Larsen, 2009). In their study, Lee & Larsen (2009) used the influence of competitors, partners and customers as an organizational property to predict the intention of SME executives (i.e., CIOs, CEOS, CFOs, and COOs) to adopt anti-malware software. Previous research has also found that SME CEOs are particularly influenced by their professional networks when making IS-related decisions (Gupta & Hammond, 2005; Ozgen & Baron, 2007). We introduced this construct in our model, as we contend that their competitors' behaviors — just like the beliefs of their customers and partners — may strongly influence CEOs' actions.

In the PMT studies using social influence (see Appendix A), this construct had a significant positive effect and, moreover, often the strongest effect on the intention to perform ISS-related actions (Ifinedo, 2012; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Siponen *et al.*, 2014; Tu *et al.*, 2015). Similarly to the threat appraisal constructs, we found no hint in the literature regarding different effects on protective or supportive actions; therefore, the following hypotheses are proposed:

H5a: Social influence exerts a positive effect on SME CEOs' protective actions in their companies.

H5b: Social influence (1) exerts a positive effect on SME CEOs' supportive actions in their companies, and (2) this effect will be similar to that on protective actions.

3.6. Control variables

Gender has been found to influence technology changes and IS acceptance (Maruping & Magni, 2012; Venkatesh *et al.*, 2000). In ISS, previous research has found that being female negatively affects actual protective behavior (Barlette *et al.*, 2017; Lee, 2011). *Firm size* is often considered in PMT studies as a relevant control variable. Barlette *et al.* (2017) found that larger firm size negatively affected protective actions. We can assume that as SMEs grow, the probability that the CEO will be helped by IT specialists may increase through the creation of internal IT positions or outsourcing because financial resources may be linked to company size. Hence, we expect a larger firm size to negatively influence protective actions and positively supportive actions. Finally, assuming that as their *level of education* increases, individuals become more aware of ISS issues, a higher education level is expected to positively influence CEOs' protective and supportive actions. In table 2, the following control variables (CVs) are proposed:

Effect / Control Variable	Effect on Protective Actions	Effect on Supportive Actions
Gender (M=0; F=1)	- (Female)	+ (Female)
Firm Size	-	+
Education	+	+

Table 2: Control variables and expected effect.

4. METHOD

4.1. Measures

We designed the questionnaire based on a review of prior literature. The questions were first pretested through face-to-face interviews with SME CEOs (N=14). Based on the CEOs' feedback, the questions' readability was improved. The final questionnaire is shown in Appendix B. All the key constructs were modeled as reflective constructs (Petter *et al.*, 2007) and were measured in the model using multiple items with 7-point Likert scales (see Appendix B), with 1=Strongly disagree and 7=Strongly agree.

For the tested dependent variables, we establish that for SME CEOs, (1) *Protective actions* correspond to taking personal charge of ISS, that is, implementing ISS measures, performing updates or backups or keeping informed about competitors' practices in ISS, while (2) *Supportive actions* correspond to CEOs validating ISS measures or validating ISS budgets proposed by the person in charge of the company's ISS (internal or external), supporting the person in charge of ISS or raising employees' awareness of ISS measures. The constructs (see table 3) were mainly borrowed or adapted from the following references (see also Appendix B for more details and psychometric scales):

Three CVs were included (see Appendix B): firm size (Size) measured as the number of employees (between 1 and 250); education measuring the education level (6 levels); and gender in the form of a dummy variable (Male: 0, Female: 1).

4.2. Data collection

The questionnaire was created using Qualtrics and submitted to 8000 SME CEOs through email. The respondents were informed that participation in the study was voluntary and that their responses would be kept confidential. The response rates for ISS-related surveys are usually low (Wolcott *et al.*, 2008). A total of 291 responses were received early in 2015. First, we removed incomplete and invalid responses. Second, all questionnaires with excessively short duration were removed, and IP addresses were used to control for duplicate submissions. This process improved the validity of the survey.

Constructs	References
Perceived severity	Siponen *et al.* (2014); Vance *et al.* (2012)
Perceived vulnerability	Ifinedo (2012); Siponen *et al.* (2014); Vance *et al.* (2012)
Self-efficacy	Ifinedo (2012); Lent *et al.* (2006); Vance *et al.* (2012)
Response efficacy	Ifinedo (2012); Vance *et al.* (2012)
Social influence	Anderson & Agarwal (2010); Lee & Larsen (2009)
Protective actions	Boss *et al.* (2015); Jarvenpaa & Ives (1991); Lai *et al.* (2012); Workman *et al.* (2008)
Supportive actions	Lee & Larsen (2009); Ragu-Nathan *et al.* (2004); Siponen *et al.* (2014); Thong *et al.* (1996)

Table 3: Constructs and references.

CEOs with no employees were removed from the sample. Finally, only respondents having access to internal or external IT resources were considered, to ensure that CEOs were able to exert both protective and supportive actions. We finally obtained 200 usable responses. The respondent profiles are presented in the descriptive statistics below.

5. DATA ANALYSIS AND RESULTS

The questionnaire was analyzed and validated through partial least squares structural equation modeling (PLS-SEM) using SMARTPLS 3.2.8. The PLS-SEM approach has a broad scope and flexibility of theory and practice (Richter *et al.*, 2016) and permits the use of small sample sizes (Hair *et al.*, 2017a) and second-order constructs (Hair *et al.*, 2017b). In addition, in large and complex models with latent variables, PLS-SEM is virtually without competition (Richter *et al.*, 2016; Wold, 2006).

5.1. Descriptive statistics

The average CEO is a 39-year-old man who has held the position for 7.5 years, and thirty-eight employees work in the average SME (N=200). The majority of respondents are male (75%). The proportion of female CEOs in the sample (25%) is similar to the European figure of 29% (European Union, 2016). In terms of company size, the sample is distributed as follows: 81 (40%) are micro-firms with fewer than ten employees, 72 (36%) employ between 10 and 49 employees, and 47 (24%) are medium-sized businesses. Appendix C provides the similarities and discrepancies among the level of protective behavior, the level of supportive behavior and the level of action according to company size. These results will be discussed in Section 6.

5.2. Overall model assessment

Bootstrapping was performed with 5,000 iterations (Hair *et al.*, 2017a; Henseler *et al.*, 2016). The approximate model fit was tested via the standardized root mean square residual (SRMR), and the overall model fit was tested via geodesic discrepancy (d_G) for protective and supportive actions (Henseler *et al.*, 2016, p. 12).

All SRMR values are under the 0.08 threshold (Henseler *et al.*, 2016), and the two estimated d_G values are equal to their saturated d_G values (see table 4). That is, the discrepancy between the empirical and the model-implied correlation matrix is not significant; therefore, our models exhibit adequate fit.

	Protective actions		**Supportive actions**	
	SRMR	d_G	SRMR	d_G
Estimated	0.059	0.373	0.052	0.360
Saturated	0.059	0.373	0.052	0.360

Table 4: Indicators of model fit.

5.3. Measurement model

5.3.1. Construct reliability and convergent validity

Appendix D exhibits composite reliabilities within the interval [0.7-0.95], indicating that they meet the "satisfactory to good" condition for construct reliability (Hair *et al.*, 2017a). The constructs' convergent validity is also adequate because all average variance extracted (AVE) values are well over 0.5, meaning that each construct explains more than 50% of the variance of its indicators (Hair *et al.*, 2011).

	Constructs' influence on **Protective Actions**				Constructs' influence on **Supportive Actions**			
	Path Coefficient	Student's Test	P Values	Signifi cance	Path Coefficient	Student's Test	P Values	Signifi cance
Vulnerability	0.164	2.395	0.017	*	0.140	1.986	0.047	*
Severity	0.046	0.741	0.459		0.198	3.132	0.002	**
Self-efficacy	0.305	4.246	0.000	***	0.135	1.974	0.048	*
Response efficacy	0.210	2.966	0.003	**	0.185	2.276	0.023	*
Social influence	0.167	2.515	0.012	*	0.243	3.404	0.001	***
Education	-0.047	0.876	0.381		-0.038	0.720	0.471	
Gender	0.082	1.347	0.178		0.057	0.934	0.351	
Firm Size	0.037	0.668	0.504		-0.048	0.822	0.411	

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

Table 5: Value and significance of path coefficients.

5.3.2. Discriminant validity

Discriminant validity was assessed through two criteria (Appendix D): all (1) heterotrait-monotrait ratios of correlations (HTMT) are smaller than 0.85 (Henseler *et al.,* 2015, 2016), and (2) 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).

5.4. Structural model analysis

Our model explains a significant amount of the variance in our endogenous variables; R^2 values are close to their adjusted values, i.e., 0.378 (0.352 adj.) for protective actions and 0.374 (0.347 adj.) for supportive actions. Bootstrapping provided the estimated t-values (Student's test) and p-values to assess path coefficient significance (table 5).

In Figure 3, the R^2 values reflect the model's in-sample predictive power (Sarstedt *et al.*, 2014). These values are satisfactory (R^2_Prot = 0.38 and R^2_Supp = 0.37) for a behavioral study (Hair *et al.,* 2011; 2017a).

Self-efficacy has a strong and significant influence and explains 31% of the CEOs' protective actions, followed by response efficacy (b=0.21), social influence (b=0.17) and perceived vulnerability (b=0.16). Neither perceived severity nor any of the CVs are significant, having a quasi-null effect. The variables with the strongest influence on supportive actions are social influence (b=0.24), perceived severity (b=0.20) and response efficacy (b=0.19). Perceived vulnerability and self-efficacy follow (b=0.14). The CVs do not exert any effect on either protective or supportive actions.

5.5. Common method bias assessment

Several means to assess and minimize common method bias were used (Podsakoff *et al.*, 2003; Straub *et al.*, 1995). First, a priori procedural remedies (Podsakoff *et al.*, 2012) were used, such as improvements to scale items to eliminate ambiguity and a mix of Likert scales with answer categories, such as yes/no, multiple choice and slider questions. Second, the marker variable approach was adopted, following the guidelines of

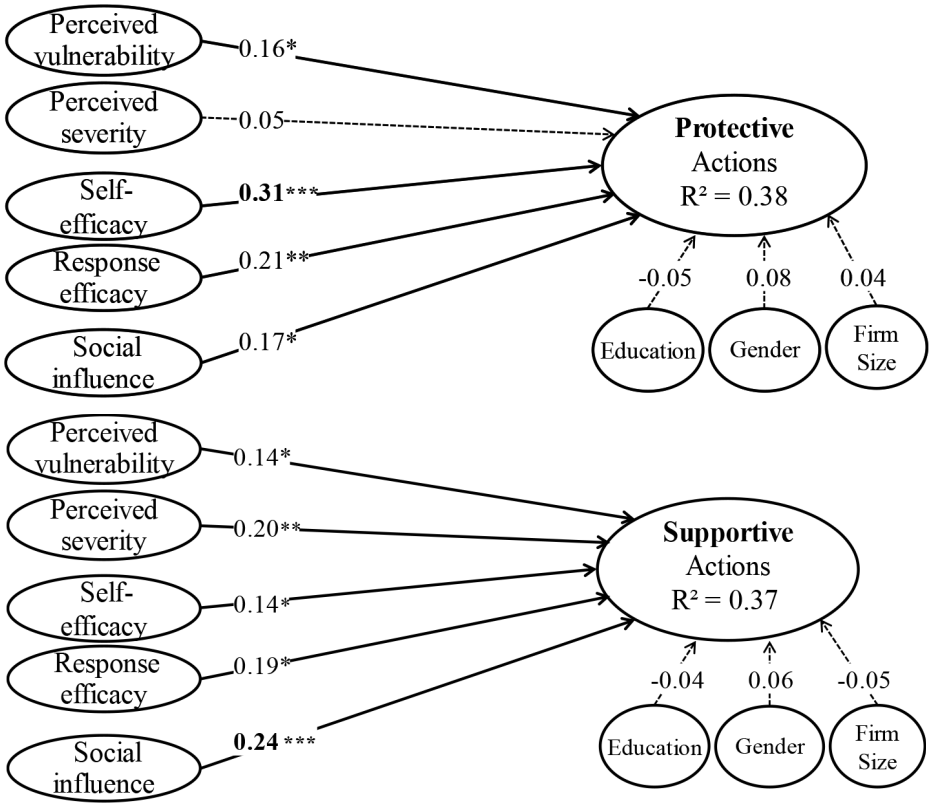

Figure 3: Comparison of results between protective and supportive actions.

Simmering *et al.* (2015, p. 476). The correlational approach described by Lindell & Whitney (2001) was used. This technique has recently been fully demonstrated to provide an overall indication of the extent to which CMV biases the results of PLS-SEM studies (Malhotra *et al.*, 2017; Schaller *et al.*, 2015). Job tenure was used as a post hoc marker variable (Simmering *et al.*, 2015), as it is theoretically uncorrelated with the variables included in the model. The results demonstrate (see Appendix E) that the maximum shared variance between the marker variable and the latent factors included in the models is 4.3%, below the threshold of 9% recommended by Tehseen *et al.* (2017). Third, several crosschecks were performed to increase the reliability of the questionnaire, and fourth, the results of the structural model demonstrated different levels of significance for the path coefficients.

6. DISCUSSION

6.1. Contrasting the determinants of SME CEOs' protective and supportive actions

The results show that our model explains a significant amount of variance for both protective (R^2=0.38) and supportive (R^2=0.37) actions. They also highlight expected and

Variables	Protective Actions	Hypothesis Validation	Supportive Actions	Hypothesis Validation	
Perceived vulnerability	0.16*	H1a: Yes	0.14*	H1b1: Yes	H1b2: Yes
Perceived severity	0.05^{NS}	H2a: No	0.20**	H2b1: Yes	H2b2: No
Self-efficacy	0.31***	H3a: Yes	0.14*	H3b1: Yes	H3b2: Yes
Response efficacy	0.21**	H4a: Yes	0.19*	H4b1: Yes	H4b2: Yes
Social influence	0.17*	H5a: Yes	0.24***	H5b1: Yes	H5b2: No

Table 6: Comparison of variable influences and hypothesis validation.

unexpected discrepancies between the determinants of SME CEOs' protective and supportive actions (see table 6).

For protective actions, all hypotheses were validated except for perceived severity, which was not significant in this study. Self-efficacy exhibited the most significant effect (0.31***), and significant results were also found concerning response efficacy (0.21**), social influence (0.17*) and perceived vulnerability (0.16*). Self-efficacy was the predominant driver of SME CEOs' protective actions, which suggests that when CEOs have positive perceptions of their behavioral efficacy, they tend to be more secure and implement ISS measures by themselves. As expected, perceived vulnerability exhibits a positive impact on protective actions (0.16*), confirming our hypothesis that for SME CEOs, the threats to their ISS remain personally relevant. These results confirm the validity of PMT and social influence on SME CEOs' protective actions.

Studying *supportive actions* provides rich insights. First, all our hypotheses for the expected effects of the constructs on supportive actions are validated. Moreover, with an R^2 of 0.37, the explanatory power of our model is satisfactory, implying that PMT can be successfully used to explain TMS. Second, the hypotheses concerning the *discrepancies between the drivers of protective and supportive actions* are partially validated (3 out of 5) and require specific attention. While we hypothesized the same effect concerning the influence of perceived severity and perceived vulnerability, only perceived vulnerability exhibits a similar effect on protective and supportive (0.16* vs. 0.14*) actions (H1b2 is validated).

The effect of perceived severity on protective actions does not appear to be significant, while its effect on supportive actions is significant and much stronger (0.05NS vs. 0.20**); hence, H2b2 is not validated. The fact that the impact of severity is not significant for protective actions may be explained by the high level of the CEOs' self-efficacy (b=0.31) to trigger these protective actions. Hence, when CEOs feel they have control over protective actions, the impacts of a security breach will not be important (self-confidence and maybe overconfidence). In contrast, perceived severity is strongly significant for supportive actions. A possible explanation for this result is that when CEOs delegate to and support another skilled person, they assume that if an ISS disaster occurs, it will have a greater impact than it would if they had taken personal charge of their company's ISS measures. This result could also illustrate a lack of confidence of CEOs in IT specialists when addressing ISS-related issues. Another explanation lies in an inversion of causality: because they fear potential severe impacts

of security breaches, CEOs outsource their company's ISS to IT specialists. Arbitrating between these two potential explanations deserves additional investigation.

As hypothesized for H3b2, self-efficacy has a lower influence on supportive actions than on protective actions (0.14* vs. 0.31***), as protective actions are more technical and need more perceived capabilities than simply providing support to the person in charge; thus, H3b2 is validated.

However, in line with what was expected, response efficacy exerts a similar effect on protective and supportive actions (0.21** vs. 0.19*); hence, H4b2 is validated.

An interesting result regards the impact of social influence (H5b2). We hypothesized a similar effect for both types of actions, but the effect on supportive actions appeared to be greater than that on protective actions (0.24*** vs. 17*). Hence, H5b2 is not validated. More importantly, social influence appears to be the main determinant of SME CEOs' supportive actions. This result is explained in greater depth in the next subsection.

6.2. Theoretical implications

This study offers several theoretical implications. First, we extend the knowledge on SME CEOs and their ISS behavior by offering new insights on the type of actions they can implement as well as on what determines these actions.

Second, this research contributes to the literature on ISS by identifying discrepancies between the determinants of SME CEOs' protective and supportive actions. This finding confirms the relevance of distinguishing the two types of behaviors, especially for small businesses. Hence, the results show that, in contrast with those of large companies, SME CEOs exert both protective and supportive behaviors (see appendix C) and that these two ways of managing ISS are influenced by distinctive triggering factors. Protective actions (i.e., when CEOs decide to implement security measures by themselves) are determined mainly by self-efficacy; however, this is much less the case for supportive actions that are more strongly impacted by social influence. These differentiated effects can also explain the discrepancies found in previous studies between the effects of the determinants on ISS behaviors: they may depend on the type of behavior (protective or supportive), on the intention vs. action, and on the population investigated (students, IT professionals, employees, and CEOs).

In appendix C, we observe that the percentage of CEOs having a high level of protective actions is the same, regardless of the size of the company (25-28%). This finding confirms studies showing that whatever the SME's size, some CEOs want to act by themselves and do not delegate managerial or IS/ISS decisions (Barber *et al.*, 2016; Jaouen & Lasch, 2015). Conversely, the share between low and medium levels of protective actions evolves from nearly 1 to 1 (37% vs. 38%) in very small SMEs to more than three times (57% vs. 17%) for large SMEs. For supportive actions, the levels evolve more gradually when the company size increases (low levels increase by 14%, while the medium and high levels decrease by 7% each). We could have assumed that as firms grow more, CEOs increase their level of supportive actions more. Nevertheless, the proportion of "high-level" supportive actions decreases as the size of the firm grows. We can then conclude (a) that the proportion of CEOs who implement protective actions by themselves is stable regardless of the size and (b) that the highest level of supportive actions is found in the smallest firms.

Third, we contribute to the knowledge on the TMS determinants in ISS by validating

the explanatory power of PMT. We validated the significant impact of five factors, namely, perceived severity, perceived vulnerability, self-efficacy, response efficacy and social influence, which exhibited the most important influence on TMS. TMS has been found to be critical for the success of ISS projects (Daud *et al.*, 2018; Hu *et al.*, 2012). Although there are many practical guidelines for enhancing TMS in ISS and many studies showing its effects on employee compliance, its drivers have almost never been investigated. This first quantitative study of TMS drivers in ISS helps address the lack of theoretically based and empirically validated research in this area.

Fourth, for SME CEOs, the main determinant of TMS is social influence. Because the theoretical background showed that SME CEOs often lack time and IS/ISS skills, we can assume that when they are aware — because of external influences — of the importance of ISS issues, it is easier for them to implement supportive actions than protective ones. Another justification could be that supportive actions are often less time-consuming and burdensome than protective actions, especially for CEOs who lack ISS skills. This strong effect of social influence shows that the professional network plays a crucial role in enhancing CEOs' actions in ISS. In this way, it would be particularly fruitful to extend the analysis of TMS determinants to other extra-organizational members of CEOs' networks and other environmental factors. This interesting result could also be put into perspective with studies about the multiple patterns of social influence (Burkhardt, 1994; Johnston & Warkentin, 2010): according to the type of actor and the pattern of relation, they can (a) follow the advice or (b) be inspired by similar behaviors of their social network actors: peers, competitors, suppliers, customers or personal networks. In this way, this study has deepened our knowledge of the ISS-related actions of CEOs and, by extension, top managers.

Finally, in accordance with Johnston *et al.* (2015), our results show that perceived vulnerability exhibits a positive impact on protective actions, confirming our hypothesis that for SME CEOs, the threats to their ISS remain personally relevant, in contrast to the case for employees. Hence, our results can challenge existing literature on this topic (for instance, Li *et al.* (2010)), as our results confirm that SME CEOs tend to identify themselves much more strongly with their firms than their employees do (Jaouen & Lasch, 2015).

6.3. Managerial implications

This study makes a number of contributions to practice. The distinction between CEOs' protective and supportive actions is critical.

In the smallest SMEs, CEOs are often alone and forced to undertake protective actions (see Figure 1). However, if necessary, CEOs can sometimes rely on other IT-skilled staff and therefore exert supportive behavior. In the largest SMEs, we found that the proportion of CEOs who exert a high level of protective measures does not vary (see Appendix C), even if the CEO is surrounded by more technicians. However, the level of supportive behavior tends to diminish. Therefore, the focus should be placed on the determinants of supportive actions, i.e., TMS, to maintain its benefits for ISS.

We found that social influence exerted the main effect on TMS. Hence, we recommend benefiting from CEOs' professional networks or their relationships with customers, suppliers, and partners. CEOs could also meet peers through social events. After social influence, TMS is similarly impacted by both threat and coping appraisals.

Perceived vulnerability and severity are matters of awareness: reports of security surveys and assessments of risks and consequences could be made available to CEOs, regardless of the size of the company. Government bodies could increase the spread of executive security reports, including actual examples of companies that experienced security breaches and their consequences, and they could provide online tools to allow easy self-assessment. CEOs could specify the features of their companies, such as their size, industry, extent of strategic activities, and turnover, on their websites to obtain an assessment of the potential risks and losses.

Coping appraisal is an important determinant of both supportive and protective behaviors. Even if self-efficacy is less important for triggering supportive actions, having knowledge of the most basic safeguards remains incontrovertible as a driver of protective behaviors (Crossler & Bélanger, 2014; Gurung *et al.*, 2009; Liang & Xue, 2010). Hence, knowledge sharing could be initiated through social exchanges (professional networks) and through interactions with technicians. Knowledge of the main problems and how they have been solved and elements of technical vocabulary could then be acquired.

In appendix C, the comparison between the levels of protective and supportive behaviors shows that when the level of protective actions is high (more than 5 out of 7), the level of supportive actions is also high for 65% of CEOs. The opposite is not true. The same can be observed for low levels of actions. We can assume that by providing support, CEOs learn from their interactions with external providers or internal IT staff (therefore increasing their awareness about dangers) and acquire technical bases through these exchanges (thus resulting in higher perceived self-efficacy).

The second element of coping appraisal, i.e., the perception of the efficacy of responses, is important for protective behaviors and could be enhanced in the same manner as self-efficacy. Supportive behaviors can be enhanced through greater confidence in the capabilities of the internal person in charge or the external technician. Therefore, building on social capital through better communication and knowledge sharing would enhance TMS for ISS projects (Liu *et al.*, 2015). For external experts, agreements or certifications could increase the necessary confidence in their skills.

6.4. Limitations and future research

Although this study provides meaningful insights, it has several limitations. First, we could not test the effects of certain CVs, such as industry type, financial resources or IT intensity. Second, the proportion of companies did not allow us to perform significant subgroup analyses, for example, addressing firm size (micro, small, medium and large) or gender influence. Replicating this study using a larger sample size would allow for such analyses. It would also be interesting to identify specific ISS-related behaviors that depend on specific demographic variables. Future studies could also integrate CVs assessing the presence of internal and/or external IT specialists. This assessment could include the number of internal/external IT specialists and, for each one, the actual time spent at work (e.g., 2 days a week) and the approximate time share between IS and ISS (e.g., 80% for IT and 20% for ISS).

Even though we included in our study the influence of peers and professional networks through social influence, a third limitation is that SME CEOs can also be socially influenced by indirectly connected peers, such as connections of connections, contacts of contacts, and friends of friends. Including this indirect social influence or

using a role equivalence model (Burkhardt, 1994) would be an interesting area for further research. Moreover, this direction would permit the assessment of a potential differentiated effect of direct and indirect social influences on protective and supportive actions. In the same vein, as CEOs can be subject to other types of organizational influences, normative and coercive forces could be investigated.

The determinants of TMS also deserve further investigation. Future research should investigate the conditions under which our findings can be extended to the top managers and CEOs of large firms. In larger companies, comparing the drivers of CEOs' protective and supportive behavior with those of other non-IT top managers would be interesting. Finally, because we could not test all supportive actions, our scales could be complemented by other items related to TMS, with a focus on various kinds of championing behaviors, for example.

Future studies should consider the type of behavior (protective or supportive), the intention vs. action and the population investigated (students, IT professionals, employees, and CEOs) because it may explain some of the discrepancies identified in the effects of PMT constructs.

This research also has implications for IS-related TMS. We suggest that other constructs borrowed from the common theories about IS acceptance and use, such as the performance expectancy related to an IS project, can contribute to TMS in IS.

Our last avenue for future research corresponds to a more dynamic vision of ISS behaviors. Recently, Karjalainen *et al.* (2019) showed that ISS behaviors can change over time and circumstances. Therefore, we advocate for conducting long-term multilevel[4] research programs (Siponen & Baskerville, 2018) including, for example, longitudinal studies and the adoption of iterative models such as the CMUA, i.e., coping model of user adaptation (Beaudry & Pinsonneault, 2005; Baillette & Barlette, 2018).

7. CONCLUSION

This study analyzed the determinants of SME CEOs' actions regarding ISS. Through the study of 200 SME CEOs, we showed the relevance of separately analyzing CEOs' protective actions and supportive actions corresponding to TMS. An important contribution of this survey is the distinction between the two types of actions. First, they are triggered and influenced by different factors. Second, not acting directly does not imply that CEOs are not concerned with ISS. Exerting supportive actions is also crucial, and better triggering TMS is critical to SMEs' ISS, especially because employees' ISS behaviors are positively influenced by their managers' behaviors and expectations (Boss *et al.*, 2009; Daud *et al.*, 2018; Hu *et al.*, 2012).

This research contributes to a body of academic literature that insists on the importance of executive involvement and TMS. Another key contribution is that this study proposes the constructs of PMT and social influence as new and powerful predictors of ISS-related supportive actions by SME CEOs.

The findings are also relevant for practitioners. Differentiated levers can be activated to enhance either protective or supportive actions, depending on the level of IT-skilled resources surrounding the CEOs. We then encourage, among other means, the usage of networks to drive CEOs to engage themselves in TMS. Ultimately, we advocate for

[4] Siponen & Baskerville (2018) propose four research levels: metalevel research, basic research, applied research, and postintervention research. The ultimate goal of such programs is to "*demonstrate the best track record of intervention rates for a given ISS problem*" (p. 259).

future research on the determinants of TMS, i.e., supportive actions in IS, which remain under researched, and especially in ISS, which have rarely been investigated to date.

ACKNOWLEDGEMENTS

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

FUNDING DETAILS

This research received support from 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).

REFERENCES

Abubakare M., Coombs C. R., Ravishankar M. N. (2017), "The Impact of Salient Cultural Practices on the Outcome of IS Implementation", *Journal of Global Information Management,* vol. 25, n°3, p. 1–20.

Almandoz J., Tilcsik A. (2016), "When Experts Become Liabilities: Domain Experts on Boards and Organizational Failure", *Academy of Management Journal,* vol. 59, n°3, p. 1124–1149.

Anderson C. L., Agarwal R. (2010), "Practicing Safe Computing: A Multimethod Empirical Examination of Computer User Security Behavioral Intentions", *MIS Quarterly,* vol. 34, n°3, p. 613–643.

Baillette P., Barlette Y. (2018), "Examining CEOs' Behavior related to BYOD implementation through the CMUA", *23rd conference of the Association Information et Management (AIM)*, May 16-18, Montréal, Canada.

Bandura A. (1977), "Self-Efficacy: Toward a Unifying Theory of Behavioral Change", *Psychological Review,* vol. 84, n°3, p. 191–215.

Bandura A. (1986), *Social Foundations of Thought and Action: A Social Cognitive Theory*, Prentice-Hall, Englewood Cliffs, NJ.

Barber J., Metcalfe S., Porteous M. (2016), *Barriers to growth in small firms*, Routledge.

Barlette Y. (2012), "Implication et Action Des Dirigeants : Quelles Pistes Pour Améliorer la Sécurité de l'Information en PME ?", *Systèmes d'Information & Management,* vol. 17, n°3, p. 115–149.

Barlette Y., Gundolf K., Jaouen A. (2017), "CEOs' Information Security Behavior in SMEs: Does Ownership Matter?", *Systèmes d'Information & Management,* vol. 22, n°3, p. 7–45.

Barlette Y., Jaouen A. (2012), "What is the Influence of Certified Public Accountants on Microfirm Owner-Managers?", in *XXVIth Research in Entrepreneurship and Small Business Conference (RENT*, Lyon, France.

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

Berry C. T., Berry R. L. (2018), "An Initial Assessment of Small Business Risk Management Approaches for Cyber Security Threats", *International Journal of Business Continuity and Risk Management,* vol. 8, n°3, p. 1–10.

Boonstra A. (2013), "How do Top Managers Support Strategic Information System Projects and Why do they Sometimes Withhold this Support?", *International Journal of Project Management,* vol. 31, n°3, p. 498–512.

Boss S. R., Galletta D. F., Lowry P. B., Moody G. D., Polak P. (2015), "What do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors", *MIS Quarterly,* vol. 39, n°3, p. 837–864.

Boss S. R., Kirsch L. J., Angermeier I., Shingler R. A., Boss R. W. (2009), "If Someone is Watching, I'll do What I'm Asked: Mandatoriness, Control, and Information Security", *European Journal of Information Systems,* vol. 18, n°3, p. 151–164.

Burkhardt M. E. (1994), "Social Interaction Effects Following a Technological Change: A Longitudinal Investigation", *Academy of Management Journal,* vol. 37, n°3, p. 869–898.

Burt R. S. (1987), "Social Contagion and Innovation: Cohesion versus Structural Equivalence", *American Journal of Sociology,* vol. 92, n°3, p. 1287–1335.

Chen Y., Ramamurthy K., Wen K.-W. (2012), "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?", *Journal of Management Information Systems,* vol. 29, n°3, p. 157–188.

Chen Y., Zahedi F. M. (2016), "Individuals' internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China", *MIS Quarterly,* vol. 40, n°3, p. 205–222.

Chu A. M. Y., Chau P. Y. K. (2014), "Development and Validation of Instruments of Information Security Deviant Behavior", *Decision Support Systems,* vol. 66, n°3, p. 93–101.

Contractor N. S., Eisenberg E. M. (1990), "Communication Networks and New Media in Organizations" in J. Fulk and C. Steinfield (eds), *Organizations and Communication Technology*, Sage, Newbury Park, CA, p. 143–172.

Crossler R., Bélanger F. (2014), "An Extended Perspective on Individual Security Behaviors", *SIGMIS Database,* vol. 45, n°3, p. 51–71.

Curran J., Burrows R. (2015), "The Social Analysis of Small Business: Some Emerging Themes" in R. Goffee and R. Scase (eds), *Entrepreneurship in Europe: The Social Processes*, Routledge, London, UK, p. 164–191.

Dagorn N., Poussing N. (2012), "Engagement et Pratiques des Organisations en Matière de Gouvernance de la Sécurité de L'information", *Systèmes d'Information & Management,* vol. 17, n°3, p. 113–143.

Daud M., Rasiah R., George M., Asirvatham D., Thangiah G. (2018), "Bridging the Gap between Organisational Practices and Cyber Security Compliance: Can Cooperation Promote Compliance in Organisations?", *International Journal of Business & Society,* vol. 19, n°3, p. 161–180.

de Guinea A. O., Kelley H., Hunter M. G. (2005), "Information Systems Effectiveness in Small Businesses", *Journal of Global Information Management,* vol. 13, n°3, p. 55–79.

Dojkovski S., Lichtenstein S., Warren M. J. (2007), "Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia", in *15th European Conference on Information Systems*, St. Gallen, Switzerland.

Dong L., Neufeld D., Higgins C. (2009), "Top Management Support of Enterprise Systems Implementations", *Journal of Information Technology,* vol. 24, n°3, p. 55–80.

Elbanna A. (2013), "Top Management Support in Multiple-Project Environments: An In-Practice View", *European Journal of Information Systems,* vol. 22, n°3, p. 278–294.

European Union. (2016), *Annual Report on European SMEs 2015-2016*, EU Publication Office, London, UK.

Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. (2016), "Decision Support Approaches for Cyber Security Investment", *Decision Support Systems,* vol. 86, n°3, p. 13–23.

Fishbein M., Ajzen I. (1975), *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Addison-Wesley Pub. Co., Reading, MA.

Floyd D. L., Prentice-Dunn S., Rogers R. W. (2000), "A Meta-Analysis of Research on Protection Motivation Theory", *Journal of Applied Social Psychology,* vol. 30, n°3, p. 407–429.

Fornell C., Larcker D. F. (1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error", *Journal of Marketing Research,* vol. 18, n°3, p. 39–50.

Friend M. A., Pagliari L. R. (2000), "Establishing a Safety Culture: Getting Started", *Professional Safety,* vol. 45, n°3, p. 30–32.

Gottschalk P. (1999), "Strategic Information Systems Planning: the IT Strategy Implementation Matrix", *European Journal of Information Systems,* vol. 8, n°3, p. 107–118.

Gupta A., Hammond R. (2005), "Information Systems Security Issues and Decisions for Small Businesses", *Information Management & Computer Security,* vol. 13, n°3, p. 297–310.

Gurung A., Luo X., Liao Q. (2009), "Consumer Motivations in Taking Action Against Spyware: An Empirical Investigation", *Information Management & Computer Security,* vol. 17, n°3, p. 276–289.

Hair J., Hollingsworth C. L., Randolph A. B., Chong A. Y. L. (2017b), "An Updated and Expanded Assessment of PLS-SEM in Information Systems Research", *Industrial Management & Data Systems,* vol. 117, n°3, p. 442–458.

Hair J. F., Hult G. T. M., Ringle C., Sarstedt M. (2017a), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage, Thousand Oaks, CA.

Hair J. F., Ringle C. M., Sarstedt M. (2011), "PLS-SEM: Indeed a Silver Bullet", *The Journal of Marketing Theory and Practice,* vol. 19, n°3, p. 139–152.

Hanus B., Wu Y. A. (2016), "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective", *Information Systems Management,* vol. 33, n°3, p. 2–16.

Henseler J., Hubona G., Ray P. A. (2016), "Using PLS Path Modeling in New Technology Research: Updated Guidelines", *Industrial Management & Data Systems,* vol. 116, n°3, p. 2–20.

Henseler J., Ringle C. M., Sarstedt M. (2015), "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling", *Journal of the Academy of Marketing Science,* vol. 43, n°3, p. 115–135.

Herath T., Rao H. R. (2009), "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems,* vol. 47, n°3, p. 154–165.

Hu Q., Dinev T., Hart P., Cooke D. (2012), "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture", *Decision Sciences,* vol. 43, n°3, p. 615–660.

Ifinedo P. (2012), "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", *Computers & Security,* vol. 31, n°3, p. 83–95.

Ismail N. (2018), SMEs: Don't Just Wait for a Security Compromise. Be Proactive. https://www.information-age.com/smes-security-compromise-123473095/. Accessed April 25, 2019.

Jaouen A., Lasch F. (2015), "A New Typology of Micro-Firm Owner-Managers", *International Small Business Journal,* vol. 33, n°3, p. 397–421.

Jaouen A., Nakara W. A. (2015), "'Bricolage' in the Implementation and the Use of IS by Micro-Firms: An Empirical Study" in Rocha, Á., Correia, A.M., Costanzo, S., Reis, L.P. (eds), *New Contributions in Information Systems and Technologies*, Springer, New York, NY, p. 449–458.

Jarvenpaa S. L., Ives B. (1991), "Executive Involvement and Participation in the Management of Information Technology", *MIS Quarterly,* vol. 15, n°3, p. 205–227.

Johnston, A. C., Hale, R. (2009), "Improved Security through Information Security Governance", *Communications of the ACM*, vol. 52, n°1, p. 126-129.

Johnston A. C., Warkentin M. (2010), "Fear Appeals and Information Security Behaviors: An Empirical Study", *MIS Quarterly,* vol. 34, n°3, p. 549–566.

Johnston A. C., Warkentin M., Siponen M. T. (2015), "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric", *MIS Quarterly,* vol. 39, n°3, p. 113–134.

Kankanhalli A., Teo H.-H., Tan B. C. Y., Wei K.-K. (2003), "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management,* vol. 23, n°3, p. 139–154.

Kanwal N., Zafar M. S., Bashir S. (2017), "The Combined Effects of Managerial Control, Resource Commitment, and Top Management Support on the Successful Delivery of Information Systems Projects", *International Journal of Project Management,* vol. 35, n°3, p. 1459–1465.

Kappelman L. A., McKeeman R., Zhang L. (2006), "Early Warning Signs of IT Project Failure: The Dominant Dozen", *Information Systems Management,* vol. 23, n°3, p. 31–36.

Karjalainen M., Sarker S., Siponen M. (2019), "Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective", *Information Systems Research,* vol. 30, n°2, p. 687-704.

Knapp K. J., Marshall T. E., Rainer R. K., Ford F. N. (2006), "Information Security: Management's

Effect on Culture and Policy", *Information Management & Computer Security,* vol. 14, n°3, p. 24–36.

Kulkarni U., Robles-Flores J., Popovi A. (2017), "Business Intelligence Capability: The Effect of Top Management and the Mediating Roles of User Participation and Analytical Decision-Making Orientation", *Journal of the Association for Information Systems,* vol. 18, n°3, p. 516–541.

Kwon J., Ulmer J. R., Wang T. (2013), "The Association between Top Management Involvement and Compensation and Information Security Breaches", *Journal of Information Systems,* vol. 27, n°3, p. 219–236.

Kyobe M. (2008), "The Impact of Entrepreneur Behaviors on the Quality of e-Commerce Security: A Comparison of Urban and Rural Findings", *Journal of Global Information Technology Management,* vol. 11, n°3, p. 58–79.

Lábodi C., Michelberger P. (2010), "Necessity or Challenge-Information Security for Small and Medium Enterprises", *Annals of the University of Petrosani Economics,* vol. 10, n°3, p. 207–216.

Lai F., Li D., Hsieh C.-T. (2012), "Fighting Identity Theft: The Coping Perspective", *Decision Support Systems,* vol. 52, n°3, p. 353–363.

Lee J. Y., Park S., Baker R. (2018), "The Moderating Role of Top Management Support on Employees' Attitudes in Response to Human Resource Development Efforts", *Journal of Management & Organization,* vol. 24, n°3, p. 369–387.

Lee Y. (2011), "Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective", *Decision Support Systems,* vol. 50, n°3, p. 361–369.

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,* vol. 18, n°3, p. 177–187.

Lent R. W., Hoffman M. A., Hill C. E., Treistman D., Mount M., Singley D. (2006), "Client-Specific Counselor Self-Efficacy in Novice Counselors: Relation to Perceptions of Session Quality", *Journal of Counseling Psychology,* vol. 53, n°3, p. 453–463.

Lewis W., Agarwal R., Sambamurthy V. (2003), "Sources of Influence on Beliefs about Information Technology Use: An Empirical Study of Knowledge Workers", *MIS Quarterly,* vol. 27, n°3, p. 657–678.

Li L., He W., Xu L., Ash I., Anwar M., & Yuan X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, vol. 45, p. 13-24.

Li H., Zhang J., Sarathy R. (2010), "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory", *Decision Support Systems,* vol. 48, n°3, p. 635–645.

Liang H., Saraf N., Hu Q., Xue Y. (2007), "Assimilation of Enterprise Systems: the Effect of Institutional Pressures and the Mediating Role of top Management", *MIS Quarterly,* vol. 31, n°3, p. 59–87.

Liang H., Xue Y. (2010), "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective", *Journal of the Association for Information Systems,* vol. 11, n°3, p. 394–413.

Limayem M., Hirt S. G., Cheung C. M. K. (2007), "How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance", *MIS Quarterly,* vol. 31, n°3, p. 705–737.

Lin T.-C., Ku Y.-C., Huang Y.-S. (2014), "Exploring Top Managers' Innovative IT (IIT) Championing Behavior: Integrating the Personal and Technical Contexts", *Information & Management,* vol. 51, n°3, p. 1–12.

Lindell M. K., Whitney D. J. (2001), "Accounting for Common Method Variance in Cross-Sectional Research Designs", *Journal of Applied Psychology,* vol. 86, n°3, p. 114–121.

Liu G., Wang E., Chua C. (2015), "Leveraging Social Capital to Obtain Top Management Support in Complex, Cross-Functional IT Projects", *Journal of the Association for Information Systems,* vol. 16, n°3, p. 707–737.

López-Muñoz J. F., Escribá-Esteve A. (2017), "An Upper Echelons Perspective on Information Technology Business Value", *European*

Research on Management and Business Economics, vol. 23, n°3, p. 173–181.

Maddux J. E., Rogers R. W. (1983), "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change", *Journal of Experimental Social Psychology,* vol. 19, n°3, p. 469–479.

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,* vol. 46, n°3, p. 193–212.

Maruping L. M., Magni M. (2012), "What's the Weather Like? The Effect of Team Learning Climate, Empowerment Climate, and Gender on Individuals' Technology Exploration and Use", *Journal of Management Information Systems,* vol. 29, n°3, p. 79–114.

McComb S. A., Kennedy D. M., Green S. G., Compton W. D. (2008), "Project Team Effectiveness: The Case for Sufficient Setup and Top Management Involvement", *Production Planning & Control,* vol. 19, n°3, p. 301–311.

Menard P., Bott G. J., Crossler R. E. (2017), "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory", *Journal of Management Information Systems,* vol. 34, n°3, p. 1203–1230.

Merhi M. I., Ahluwalia P. (2015), "Top Management can Lower Resistance toward Information Security Compliance", in *Thirty Sixth ICIS Conference*, Fort Worth, Texas.

Mitchell J. R., Shepherd D. A. (2010), "To Thine Own Self be True: Images of Self, Images of Opportunity, and Entrepreneurial Action", *Journal of Business Venturing,* vol. 25, n°3, p. 138–154.

Moody G. D., Siponen M., Pahnila S. (2018), "Toward a Unified Model of Information Security Policy Compliance", *MIS Quarterly,* vol. 42, n°3, p. 285–311.

Mullins J. W., Forlani D. (2005), "Missing the Boat or Sinking the Boat: A Study of New Venture Decision Making", *Journal of Business Venturing,* vol. 20, n°3, p. 47–69.

Mwagwabi F., McGill T., Dixon M. (2018), "Short-Term and Long-Term Effects of Fear Appeals in Improving Compliance with Password Guidelines", *Communications of the Association for Information Systems,* vol. 42, n°3, p. 147–192.

Ng B.-Y., Kankanhalli A., Xu Y. (2009), "Studying Users' Computer Security Behavior: A Health Belief Perspective", *Decision Support Systems,* vol. 46, n°3, p. 815–825.

Nguyen T. H., Newby M., Macaulay M. J. (2015), "Information Technology Adoption in Small Business: Confirmation of a Proposed Framework", *Journal of Small Business Management,* vol. 53, n°3, p. 207–227.

Nice S. (2018), Protecting SMEs from the Evolving Threat Landscape. https://www.scmagazineuk.com/protecting-smes-evolving-threat-landscape/article/1472907/. Accessed April 25, 2019.

Ozgen E., Baron R. A. (2007), "Social Sources of Information in Opportunity Recognition: Effects of Mentors, Industry Networks, and Professional Forums", *Journal of Business Venturing,* vol. 22, n°3, p. 174–192.

Pérès A., Latour R., Bergeron J. (2003), "Attitude des Utilisateurs de Systèmes à l'égard de la Protection des Informations : Un Modèle des Facteurs d'influence", *Systèmes d'Information & Management,* vol. 8, n°3, p. 87–118.

Petter S., Straub D., Rai A. (2007), "Specifying Formative Constructs in Information Systems Research", *MIS Quarterly,* vol. 31, n°3, p. 623–656.

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", *Journal of Applied Psychology,* vol. 88, n°3, p. 879–903.

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,* vol. 63, n°3, p. 539–569.

Posey C., Roberts T. L., Lowry P. B. (2015), "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets", *Journal of Management Information Systems,* vol. 32, n°3, p. 179–214.

Prentice-Dunn S., Rogers R. W. (1986), "Protection Motivation Theory and Preventive Health:

Beyond the Health Belief Model", *Health Education Research,* vol. 1, n°3, p. 153–161.

Pritchard S. (2010), "Navigating the Black Hole of Small Business Security", *Infosecurity,* vol. 7, n°3, p. 18–21.

Puhakainen P., Siponen M. (2010), "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study", *MIS Quarterly,* vol. 34, n°3, p. 757–778.

Ragu-Nathan B. S., Apigian C. H., Ragu-Nathan T. S., Tu Q. (2004), "A Path Analytic Study of the Effect of Top Management Support for Information Systems Performance", *Omega,* vol. 32, n°3, p. 459–471.

Rainer R. K., Marshall T. E., Knapp K. J., Montgomery G. H. (2007), "Do Information Security Professionals and Business Managers View Information Security Issues Differently?", *Information Systems Security,* vol. 16, n°3, p. 100–108.

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,* vol. 34, n°3, p. 589–597.

Rogers R. W. (1983), "Cognitive and Psychological Processes in Fear-Based Attitude Change: A Revised Theory of Protection Motivation" in J. Cacioppo and R. Petty (eds), *Social Psychophysiology: A Sourcebook*, Guilford Press, New York, NY, p. 153–176.

Rondeau, P. J., Ragu-Nathan, T. S., Vonderembse, M. A. (2006), "How involvement, IS management effectiveness, and end-user computing impact IS performance in manufacturing firms", *Information & Management*, vol. 43, n°1, p. 93–107.

Rothrock R. A., Kaplan J., van der Oord F. (2018), "The Board's Role in Managing Cybersecurity Risks", *MIT Sloan Management Review,* vol. 59, n°3, p. 12–15.

Sarstedt M., Ringle C. M., Smith D., Reams R., Hair J. F. (2014), "Partial Least Squares Structural Equation Modeling (PLS-SEM): A Useful Tool for Family Business Researchers", *Journal of Family Business Strategy,* vol. 5, n°3, p. 105–115.

Schaller T. K., Patil A., Malhotra N. K. (2015), "Alternative Techniques for Assessing Common Method Variance", *Organizational Research Methods,* vol. 18, n°3, p. 177–206.

Schoonjans B., van Cauwenberge P., Bauwhede H. V. (2013), "Formal Business Networking and SME Growth", *Small Business Economics,* vol. 41, n°3, p. 169–181.

Senyard J. M., Baker T., Davidsson P. (2011), "Bricolage as a Path to Innovation for Resource Constrained New Firms", *Academy of Management Proceedings,* vol. 2011, n°3, p. 1–5.

Shao Z., Feng Y., Hu Q. (2016), "Effectiveness of Top Management Support in Enterprise Systems Success: A Contingency Perspective of Fit between Leadership Style and System Life-Cycle", *European Journal of Information Systems,* vol. 25, n°3, p. 131–153.

Shao Z., Feng Y., Hu Q. (2017), "Impact of Top Management Leadership Styles on ERP Assimilation and the Role of Organizational Learning", *Information & Management,* vol. 54, n°3, p. 902–919.

Shepherd D. A., Williams T. A., Patzelt H. (2015), "Thinking about Entrepreneurial Decision Making: Review and Research Agenda", *Journal of Management,* vol. 41, n°3, p. 11–46.

Simmering M. J., Fuller C. M., Richardson H. A., Ocal Y., Atinc G. M. (2015), "Marker Variable Choice, Reporting, and Interpretation in the Detection of Common Method Variance", *Organizational Research Methods,* vol. 18, n°3, p. 473–511.

Siponen M., Baskerville R. (2018), "Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example", *Journal of the Association for Information Systems,* vol. 19, n°4, p. 247-265.

Siponen M., Mahmood M. A., Pahnila S. (2014), "Employees' Adherence to Information Security Policies: An Exploratory Field Study", *Information & Management,* vol. 51, n°3, p. 217–224.

Siponen M., Pahnila S., Mahmood M. A. (2010), "Compliance with Information Security Policies: An Empirical Investigation", *Computer,* vol. 43, n°3, p. 64–71.

Staehr L. (2010), "Understanding the Role of Managerial Agency in Achieving Business Benefits from ERP Systems", *Information Systems Journal,* vol. 20, n°3, p. 213–238.

Štemberger M.I., Manfreda A., Kovačič A. (2011), "Achieving Top Management Support with Business Knowledge and Role of IT/IS Personnel", *International Journal of Information Management,* vol. 31, n°3, p. 428–436.

Straub D., Limayem M., Karahanna-Evaristo E. (1995), "Measuring System Usage: Implications for IS Theory Testing", *Management Science,* vol. 41, n°3, p. 1328–1342.

Tehseen S., Ramayah T., Sajilan S. (2017), "Testing and Controlling for Common Method Variance: A Review of Available Methods", *Journal of Management Sciences,* vol. 4, n°3, p. 142–168.

Thompson N., McGill T. J., Wang X. (2017), "'Security Begins at Home': Determinants of Home Computer and Mobile Device Security Behavior", *Computers & Security,* vol. 70, n°3, p. 376–391.

Thong J. Y. L., Yap C.-S., Raman K. S. (1996), "Top Management Support, External Expertise and Information Systems Implementation in Small Businesses", *Information Systems Research,* vol. 7, n°3, p. 248–267.

Torres O., Julien P. A. (2005), "Specificity and Denaturing of Small Business", *International Small Business Journal,* vol. 23, n°3, p. 355–377.

Tsai H.-Y. S., Jiang M., Alhabash S., LaRose R., Rifon N. J., Cotten S. R. (2016), "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective", *Computers & Security,* vol. 59, n°3, p. 138–150.

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,* vol. 52, n°3, p. 506–517.

Vance A., Siponen M., Pahnila S. (2012), "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory", *Information & Management,* vol. 49, n°3, p. 190–198.

Venkatesh V., Morris M. G., Ackerman P. L. (2000), "A Longitudinal Field Investigation of Gender Differences in Individual Technology Adoption Decision-Making Processes", *Organizational Behavior and Human Decision Processes,* vol. 83, n°3, p. 33–60.

Venkatesh V., Morris M. G., Davis G. B., Davis F. D. (2003), "User Acceptance of Information Technology: Toward a Unified View", *MIS Quarterly,* vol. 27, n°3, p. 425–478.

Warkentin M., Johnston A. C., Shropshire J., Barnett W. D. (2016), "Continuance of Protective Security Behavior: A Longitudinal Study", *Decision Support Systems,* vol. 92, n°3, p. 25–35.

Williams C. K., Wynn D., Madupalli R., Karahanna E., Duncan B. K. (2014), "Explaining Users' Security Behaviors with the Security Belief Model", *Journal of Organizational and End User Computing,* vol. 26, n°3, p. 23–46.

Wolcott P., Kamal M., Qureshi S. (2008), "Meeting the Challenges of ICT Adoption by Micro-Enterprises", *Journal of Enterprise Information Management,* vol. 21, n°3, p. 616–632.

Wold H. (2006), "Partial Least Squares" in S. Kotz and N. L. Johnson (eds), *Encyclopedia of Statistical Sciences*, John Wiley, New York, NY, p. 581–591.

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,* vol. 24, n°3, p. 2799–2816.

Yazdanmehr A., Wang J. (2016), "Employees' Information Security Policy Compliance: A Norm Activation Perspective", *Decision Support Systems,* vol. 92, n°3, p. 36–46.

Yoon C., Kim H. (2013), "Understanding Computer Security Behavioral Intention in the Workplace", *Information Technology & People,* vol. 26, n°3, p. 401–419.

Zafar H., Ko M. S., Osei-Bryson K.-M. (2016), "The Value of the CIO in the Top Management Team on Performance in the Case of Information Security Breaches", *Information Systems Frontiers,* vol. 18, n°3, p. 1205–1215.

Zhang B., Pavlou P. A., Krishnan R. (2018), "On Direct vs. Indirect Peer Influence in Large Social Networks", *Information Systems Research,* vol. 29, n°3, p. 292–314.

APPENDIXES

APPENDIX A: THE 29 PREVIOUS STUDIES USING PMT AND THEIR MAIN CONSTRUCTS

Authors	Year	Sample	Determinants of ISS-related actions						Dependent Variables		
			Perceived Severity	Perceived Vulnerability	Response Efficacy	Self Efficacy	Response Cost	Social Influence	Behavioral Intention	Protective Actions	Supportive Actions
Workman et al.	2008	Employees, Large IT firm	+	+	+	+	+			X	
Gurung et al.	2009	Students	+	NS	+	+	NS			X	
Herath & Rao	2009	Employees, All Sizes		NS		+		+	X		
Lee & Larsen	2009	SME executives (60% IT)	+	+	+	+	+	+	X	X	
Ng et al.	2009	Employees, All sizes	NS	+		+				X	
Anderson & Agarwal	2010	Public users and students	+		+	+		NS	X		
Johnston & Warkentin	2010	Faculty, staff and students	-	NS	+	+		+	X	X	
Liang & Xue	2010	Students	+	+	+	+	+		X	X	
Siponen et al.	2010	Employees, large companies	+		NS	+		+	X	X	
Lee	2011	Faculty	+	+	+	+	+	NS	X	X	
Ifinedo	2012	Employees, All sizes	-	+	+	+	NS	+	X		
Vance et al.	2012	Administrative, City Govt	+	NS	-	+	+		X		
Yoon & Kim	2013	Employees, All Sizes	+	NS	+	+		NS	X		
Crossler & Belanger	2014	Students and citizens	+	-	+	+	NS			X	
Siponen et al.	2014	Employees, All sizes	+	+	NS	+	NS	+	X	X	
Boss et al.	2015	Students	+	NS	NS	NS	+		X	X	
Johnston et al.	2015	Employees, City Govt	+	NS	+	+			X		
Posey et al.	2015	Employees	+		+		NS			X	
Tu et al.	2015	Public users	+		+	+		+	X		
Chen & Zahedi	2016	Individuals	+	+	+	+				X	
Hanus & Wu	2016	Students	NS	NS	+	+	NS			X	
Tsai et al.	2016	eCommerce users	-	NS	+	-	+	+	X		
Warkentin et al.	2016	Students	+	+	NS	+			X	X	
Barlette et al.	2017	SME CEOs	NS	NS	+	+	-	+	X	X	
Menard et al.	2017	Home users and employees	NS	NS	+	NS	NS		X		
Thompson et al.	2017	Home computer users	NS	+	NS	+	+	NS	X	X	
Moody et al.	2018	Working professionals	NS	-	NS	-			X		
Mwagwabi et al.	2018	Internet users	NS	NS	+	+	NS		X	X	
Li et al.	2019	Employees	NS	+	+	+	+			X	
Authors (Protective)		SME CEOs	NS	+	+	+		+		X	
Authors (Supportive)		SME CEOs	+	+	+	+		+			X

NS: Non-significant; *-: Opposite effect*

NB: Siponen *et al.* (2014) conducted the sole study addressing supportive actions, but in their analysis, they did not distinguish these behaviors from protective actions.

APPENDIX B: VARIABLES, ITEMS AND CODES

Variable		Reference	Item	Scale	Code
Threat Appraisal	Perceived severity	Vance et al., 2012; Siponen et al., 2014	If I lost my computerized data, there would be serious problems for my organization.	L7	PSEV1
			If my computerized data were temporarily not available, serious information security problems would result.	L7	PSEV2
			An information security breach would have a serious negative impact for my company.	L7	PSEV3
	Perceived vulnerability	Vance et al., 2012; Ifinedo, 2012; Siponen et al., 2014	An information security problem could occur if I did not apply security policies.	L7	PVUL1
			My personal data could be subject to a threat if I did not apply information security policies.	L7	PVUL2
			My company could be subject to a threat if I did not apply information security policies.	L7	PVUL3
Coping Appraisal	Response efficacy	Vance et al., 2012; Ifinedo, 2012	If I implement information security measures in my company, it will keep IS security breaches down.	L7	REFF1
			If I take charge of information security in my company, it will limit the impact of an information security problem.	L7	REFF2
		Vance et al., 2012	Even if I complied with information security policies, information security problems could not be avoided (Reverse-coded item).	L7	REFF3 Dropped
	Self-efficacy	Vance et al., 2012; Ifinedo, 2012	I can implement information security measures by myself.	L7	SEFF1
			Implementing information security measures is easy for me.	L7	SEFF2
		Lent et al. 2006; Ifinedo, 2012	I have the capability to solve problems during the implementation of security measures.	L7	SEFF3
Social Influence		Lee & Larsen, 2009; Anderson & Agarwal, 2010	My competitors have adopted or are in the process of adopting information security measures.	L7	SINFL1
			My partner companies believe I should adopt information security measures.	L7	SINFL2
			My customers believe I should adopt information security measures to protect their own customer data.	L7	SINFL3
Protective Actions		Rondeau et al., 2006; Workman et al., 2008 Yoon & Kim, 2013	I have personally implemented information security measures in my company (passwords, backups, updates, etc.).	L7	PROT1
		Lai et al., 2012; Liang & Xue, 2010; Boss et al., 2015	I regularly perform antivirus updates or backups in my company.	L7	PROT2
		Jarvenpaa & Ives, 1991	I get some information about my competitors' practices concerning information security.	L7	PROT3
Supportive Actions		Johnston & Hale, 2009; Thong et al., 1996	I regularly validate the IS security measures proposed by the person in charge of my company's ISS (I am not the person in charge).	L7	SUP1
		Boonstra, 2013; Lee & Larsen, 2009; Thong et al., 1996	I regularly validate the IS security budgets proposed by the person in charge of my company's ISS (I am not the person in charge).	L7	SUP2
		Stemberger et al., 2011; Ragu-Nathan et al., 2004	I regularly support the person in charge of my company's ISS (I am not the person in charge).	L7	SUP3
		Siponen et al., 2014; Posey et al., 2015	I regularly raise my employees' awareness of IS security measures.	L7	SUP4
Control Variables	Education	Ifinedo, 2012; Johnston et al., 2015	1: Self-taught; 2: NVQ1-2; 3: A level; 4: Higher educ.; 5 BA/BS; 6: MS/MA and higher	1 to 6	EDUC
	Gender	Venkatesh et al., 2003; Chen & Zahedi, 2016	Male =0; Female =1	0/1	GEND
	Firm Size	Ifinedo, 2012; Lee & Larsen, 2009	Number of employees	Num	SIZE
Marker Variable	Job Tenure	Crossler & Belanger, 2014; Siponen et al., 2014	Number of years in the position	Num	TENURE

NB: REFF3 was not included in the analyses because of poor psychometric properties.

APPENDIX C: SUPPORTIVE AND PROTECTIVE BEHAVIORS BY LEVEL AND BY COMPANY SIZE

Supportive and protective behaviors by level

		Protective behaviors			Total
		Low [1-3]	Medium]3-5[	High [5-7]	
Supportive behaviors	Low [1-3]	50	16	5	71
		56%	28%	10%	36%
	Medium]3-5[	23	26	13	62
		26%	45%	25%	31%
	High [5-7]	17	16	34	67
		19%	28%	65%	34%
Total		90	58	52	200
		100%	100%	100%	100%

The levels correspond to the average of the items measuring each type of behavior. We used Likert scales; therefore, the levels are between 1 and 7.

Supportive and protective behaviors by company size

Size	Level of action	Supportive		Protective		Total
Micro 0-9	Low	25	31%	30	37%	81
	Medium	26	32%	31	38%	
	High	30	37%	20	25%	
Small 10-49	Low	25	35%	33	46%	72
	Medium	23	32%	19	26%	
	High	24	33%	20	28%	
Medium 50-250	Low	21	45%	27	57%	47
	Medium	12	25%	8	17%	
	High	14	30%	12	26%	

APPENDIX D: CONSTRUCT RELIABILITY, CONVERGENT AND DISCRIMINANT VALIDITY

Composite reliability, average variance extracted and the Fornell-Larcker criterion

	Composite Reliability	Average Variance Extracted	Perceived vulnerability	Perceived severity	Self-efficacy	Response efficacy	Social influence	**Protective Actions**
Perceived vulnerability	0.925	0.805	**0.897**					
Perceived severity	0.882	0.713	0.607	**0.845**				
Self-efficacy	0.927	0.808	0.168	0.101	**0.899**			
Response efficacy	0.953	0.910	0.380	0.304	0.372	**0.954**		
Social influence	0.894	0.739	0.358	0.278	0.132	0.281	**0.859**	
Protective Actions	0.826	0.613	0.390	0.286	0.444	0.452	0.342	**0.783**

	Composite Reliability	Average Variance Extracted	Perceived vulnerability	Perceived severity	Self-efficacy	Response efficacy	Social influence	**Supportive Actions**
Perceived vulnerability	0.926	0.806	**0.898**					
Perceived severity	0.881	0.711	0.612	**0.843**				
Self-efficacy	0.926	0.808	0.166	0.098	**0.899**			
Response efficacy	0.953	0.910	0.380	0.302	0.372	**0.954**		
Social influence	0.896	0.741	0.360	0.279	0.134	0.280	**0.861**	
Supportive Actions	0.930	0.769	0.442	0.420	0.281	0.426	0.420	**0.877**
Validity Conditions	> 0.7	> 0.5	The diagonal represents the square root of AVE values Square root of AVE > higher correlation with other constructs					

Discriminant validity: Heterotrait-monotrait (HTMT) ratio of correlations

	Vulnerability	Severity	Self-efficacy	Response efficacy	Social influence	**Protective Actions**	Education	Gender	Size
Vulnerability									
Severity	0.716								
Self-efficacy	0.189	0.122							
Response efficacy	0.427	0.356	0.415						
Social influence	0.412	0.322	0.155	0.318					
Protective Actions	0.493	0.381	0.571	0.575	0.432				
Education	0.037	0.063	0.060	0.068	0.034	0.024			
Gender	0.042	0.041	0.103	0.152	0.077	0.176	0.109		
Size	0.062	0.028	0.031	0.083	0.088	0.117	0.029	0.148	

	Vulnerability	Severity	Self-efficacy	Response efficacy	Social influence	**Supportive Actions**	Education	Gender	Size
Vulnerability									
Severity	0.716								
Self efficacy	0.189	0.122							
Response efficacy	0.427	0.356	0.415						
Social influence	0.412	0.322	0.155	0.318					
Supportive Actions	0.494	0.481	0.313	0.472	0.472				
Education	0.037	0.063	0.060	0.068	0.034	0.028			
Gender	0.042	0.041	0.103	0.152	0.077	0.120	0.109		
Size	0.062	0.028	0.031	0.083	0.088	0.079	0.029	0.148	
Validity Threshold	**< 0.85**								

APPENDIX E: CORRELATIONS BETWEEN THE MARKER VARIABLE AND LATENT VARIABLES

	Vulnerability	Severity	Self-efficacy	Response efficacy	Social influence	**Protective Actions**	Marker Variable
Vulnerability							
Severity	0.527						
Self-efficacy	0.127	0.112					
Response efficacy	0.380	0.281	0.288				
Social influence	0.328	0.220	0.088	0.277			
Protective Actions	0.411	0.276	0.361	0.450	0.304		
Marker Variable	0.137	0.148	0.039	0.100	0.090	0.177	

Highest squared correlation: $0.177^2 = 3.1\%$

	Vulnerability	Severity	Self-efficacy	Response efficacy	Social influence	**Supportive Actions**	Marker Variable
Vulnerability							
Severity	0.527						
Self-efficacy	0.127	0.112					
Response efficacy	0.380	0.281	0.288				
Social influence	0.328	0.220	0.088	0.277			
Supportive Actions	0.429	0.375	0.234	0.422	0.400		
Marker Variable	0.137	0.148	0.039	0.100	0.090	0.208	

Highest squared correlation: $0.208^2 = 4.3\%$