CEOs' information security behavior in SMEs: Does ownership matter?

Yves BARLETTE, Katherine GUNDOLF & Annabelle JAOUEN

Montpellier Business School – Montpellier Research in Management (MRM)

ABSTRACT

Past research in the area of behavioral information security has mainly focused on large company employees. However, SMEs constitute a relevant field of study, as they represent more than 99 percent of European companies and are subject to rapidly increasing security threats. In addition, within SMEs, CEOs play a vital role in protecting their information through the actions they can initiate and the influence they have on their employees. We attempt to fill a gap in information security (ISS) research, as few studies have aimed to understand CEOs' behaviors related to the implementation of ISS. In addition, the literature shows that particularly in a small firm context, ownership influences CEOs' behavior. Even less research has addressed SMEs, specifically with regard to the impact of ownership on CEOs' ISS-related behaviors. This paper details an empirical study based on the protection motivation theory (PMT) to investigate the following research question: what factors explain SME CEOs' information security protective behavior? *We conducted a questionnaire-based survey with 292 SME CEOs, and we analyzed the collected data using partial least squares (PLS). Because the academic literature shows that SME CEOs engage in specific behaviors, we tested the influence of the PMT on two subgroups: SME owners (n=183) and non-owners (n=109). Our results show very important and significant discrepancies between the two subgroups. Our work is original because it constitutes the first study dedicated to the protective behaviors of SME CEOs; moreover, it distinguishes between owners and non-owners. Our major theoretical contribution corresponds to the identification and investigation of this differentiated population, which requires more in-depth studies. The main managerial implication of our work is that as the factors triggering owner and non-owner SME CEOs protective behaviors are almost in total contrast, any communication or action should be specifically tailored to each audience.*

Keywords: *Protection motivation theory, owner CEO, SME, behavior, information security.*

RÉSUMÉ

Jusqu'à présent, la recherche dans le domaine des comportements en sécurité de l'information a été majoritairement centrée sur les employés de grandes entreprises. Cependant, les PME constituent un champ d'études pertinent car elles représentent plus de 99% des entreprises en Europe et font face à des menaces en forte croissance touchant à leur sécurité. De plus, les dirigeants de PME jouent un rôle vital dans la protection des informations, au travers des actions qu'ils peuvent mettre en œuvre ou l'influence qu'ils ont sur leurs employés. Nous visons à contribuer à la recherche en sécurité de l'information, car peu d'études se sont intéressées aux comportements des dirigeants, relatifs à la mise en place de mesures de protection de l'information. De plus, la littérature académique a montré que, particulièrement dans un contexte de PME, le fait que le dirigeant soit propriétaire à une influence sur ses comportements. Les études portant sur les PME sont encore plus rares, d'autant plus si l'on s'intéresse à l'influence de la propriété sur les comportements des dirigeants en matière de sécurité de l'information. Ce papier présente une recherche empirique basée sur la théorie de la motivation à la protection (PMT) qui traite de la question de recherche suivante : « Quels facteurs peuvent expliquer les comportements relatifs à la protection des informations des dirigeants de PME ? *» Nous avons mené une étude auprès de 292 dirigeants de PME, les données collectées ont été analysées par la méthode des moindres carrés partiels (PLS). La littérature académique ayant montré que le comportement des dirigeants de PME est spécifique, nous avons testé l'influence de la PMT sur deux sous-populations : les dirigeants propriétaires (n=183) et non-propriétaires (n=109). Nos résultats mettent en évidence des différences très importantes et significatives entre ces deux sous-groupes. L'originalité de notre travail tient au fait qu'il constitue la première étude dédiée aux comportements des dirigeants de PME en matière de protection des informations, distinguant de plus les propriétaires des non-propriétaires. Notre principale contribution théorique correspond à la mise en évidence et à l'étude de cette population différenciée, à approfondir dans de futures recherches. L'implication managériale majeure de notre travail est que, comme les facteurs qui sont à la base des comportements de protection des dirigeants-propriétaires sont presque en contraste total comparés à ceux des dirigeants non-propriétaires, toute communication ou action devrait être spécifiquement adaptée à chacune de ces deux populations.*

Mots-clés : *Théorie de la motivation à la protection, propriétaire-dirigeant, PME, comportement, sécurité de l'information.*

1. INTRODUCTION

According to PWC (2014), the number of information security breaches in SMEs increased by 64 percent from 2013 to 2014. More than half of small businesses have been victims of cyberattacks (Keeper, 2016), and 62 percent of the attacks specifically targeted small businesses (IBM, 2016). The main reason for these attacks is that SMEs have weaker defenses than larger companies (lack of expertise, dated security defenses, outsourcing to unqualified companies), and SMEs may also serve as a way to reach larger companies' data, as SME security breaches are increasingly viewed as stepping stones for access to data at larger organizations. However, despite this reality, many SMEs still believe that they are not vulnerable to cyberattacks because of their small size and limited assets (Prnewswire, 2015).

Many threats to information security (ISS) in general can be traced to employee behavior that does not comply with information security policies (Chu & Chau, 2014; Siponen *et al.*, 2014), ISS organizational rules or even firm guidelines or requirements (Ifinedo, 2012; Workman *et al.*, 2008). Employee training and education are also important (Dagorn, 2008) because most hacking episodes occur when employees click on malicious links or websites (Gustke, 2016).

Numerous surveys have confirmed that managerial support is essential to obtaining employee adherence to ISS (Barlette *et al.*, 2015; Johnston & Hale, 2009). For example, Hu *et al.* (2012) and Puhakainen and Siponen (2010) showed that top management participation is of utmost importance in shaping employee behavior with regard to information security policy compliance. In addition, employees' involvement and propensity to act may also be directly dependent on managers' concrete actions (Dong *et al.*, 2009; Forcht & Ayers, 2001; Pérès *et al.*, 2003). For these reasons, many scholars have advocated that ISS should be addressed at the top management level (Friend & Pagliari, 2000; Knapp *et al.*, 2006).

The MIS literature has repeatedly shown that managers must not only be aware but must also be personally involved in ISS because their involvement is essential to the implementation, maintenance and success of their employees' ISS-related behaviors (Johnston & Hale, 2009). Top managers, especially CEOs, must be considered the starting point for satisfactory ISS (Robinson & Volonino, 2004). However, some CEOs are scarcely involved and/or insufficiently manage their company's ISS, leading to potentially disastrous consequences. This is particularly true for SMEs (Lábodi & Michelberger, 2010; Lee & Larsen, 2009), in which CEOs often have difficulties accessing, treating and protecting information. Regarding the importance of this topic, to date, little attention has been paid to the CEO's role in information security implementation. In fact, only a few studies have aimed to understand CEOs' participation and behaviors in ISS (Barlette, 2012; Dong, 2008; Lee & Larsen, 2009; Zwikael, 2008), and only one study specifically examined CEOs' ISS behavior in SMEs.

The SME literature highlights a certain characteristic of SME CEOs: Due to their size, SMEs are often managed by their owners (Torrès & Julien, 2005). Ownership may introduce behavioral differences in the context of firms (De Massis *et al.*, 2015; Michaelas *et al.*, 1999). Such behavioral differences are highlighted by the agency theory, for example (Jensen & Meckling, 1976; Ross, 1973). In addition, the literature on SMEs shows that particularly in the small firm context, ownership influences CEOs' behavior (i.e., Anderson & Reeb, 2003;

James, 1999; Miller *et al.*, 2008). However, little research has addressed the ISS behavior of SME CEOs, and by extension, there has been even less research with regard to the ownership of these firms.

To overcome this gap, we formulate our research question as follows: *what factors explain SME CEOs' information security protective behavior?* In addition, we examine the extent to which *the ownership of a company* affects SME CEOs' information security protective behavior.

To predict an individual's intention to engage in protective behaviors, the protection motivation theory (PMT) constitutes one of the most powerful explanatory theories (Anderson & Agarwal, 2010), and it has been widely used in ISS research (Boss *et al.*, 2015; Lee & Larsen, 2009; Liang & Xue, 2010). Hence, in this study, we use the PMT to test the factors that explain SME CEOs' behavioral intention and actual behavior when engaging in protective ISS measures.

This paper is structured as follows: in section two, we define our theoretical framework and present our literature review. In section three, we present our research model and develop our hypotheses. Section four introduces the adopted methodology by presenting our research design, variables and data analysis. We present our results in section five and discuss them in section six to outline our contributions and provide avenues for future research. In the conclusion section, we summarize our main results.

2. LITERATURE REVIEW

We first address the ISS behavior of SME CEOs, and we then present our theoretical framework: the protection motivation theory, its origins and its applications in ISS research.

2.1. SME CEOs and Information Security

2.1.1. The role of top managers in information security

Because information is a strategic resource (Rockart & Crescenzi, 1984), one of the key roles of CEOs is to define the desired balance between the cost of ISS measures and the possible productivity losses (Reid & Gilbert, 2009) based on the company's activities (Johnston & Hale, 2009). Friend and Pagliari (2000) confirmed this important role: "*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).

Strategic and financial aspects are not the only concerns: the whole company itself, including human aspects, must also be considered. From this perspective, Dutta and McCrohan (2002) highlighted the role of top management in adopting desirable organizational characteristics to achieve satisfactory information security. By virtue of their role, top managers have the ability to act as change agents in order to create a favorable environment (Kankanhalli *et al.*, 2003; Lucas, 1981). It has also been demonstrated that top managers have the necessary authority to influence employees, thus permitting them to overcome organizational resistance (Boss *et al.*, 2009; Dutta & McCrohan, 2002; Knapp *et al.*, 2006; Markus, 1983). Top management participation also has a strong effect on employees' compliance with an information security policy (Hu *et al.*, 2012; Pérès *et al.*, 2003; Puhakainen & Siponen, 2010). Therefore, top managers are able to implement the necessary rules and processes for ISS management and provide the bases of a coherent ISS approach (Bruce & Dempsey, 1997; Vermeulen & Solms, 2002). According to

Ashenden (2008), the person in charge of ISS must be a part of the company's top managers because he/she must have the necessary entrepreneurial skills to be able to act in a proactive manner as a change agent. It is up to the top managers to take on the ISS-related behavioral aspects and processes that must be complied with (Boss *et al.*, 2009). In medium and large organizations, the top managers in charge of ISS also have technical competences to successfully implement the protection measures (Vermeulen & Solms, 2002), but this is seldom the case of SMEs, where the hierarchical line is little or not at all developed and where the CEO is often not technically skilled enough to make ISS decisions (Barlette, 2008, 2012).

Therefore, CEOs ISS behavior in SMEs should be considered in detail, as it represents several specificities (Cragg *et al.*, 2011).

2.1.2. ISS behavior of SME CEOs

The literature on information systems in SMEs considers that SME CEOs exhibit specific behaviors in comparison to large companies' CEOs (Cragg *et al.*, 2011; Poutziouris, 2003). Because of their size, small firms have simple structures and processes (Cragg *et al.*, 2011; Torrès & Julien, 2005). This simplicity is reflected by a strong presence of intuition and affect in decision-making, a structural lack of resources (including time and financial resources), a flat or absent hierarchy, low formalization, oral and informal communication, and an essential versatility (Bhattacharya, 2011; Julien, 1990). There is also an alignment between the personal views of SME CEOs and their strategic and organizational behavior (Jaouen & Lasch, 2015; Mills & Pawson, 2012). Considering these constraints, SME CEOs make decisions with a short-term vision, often reactively or based on limited information (Torrès & Julien, 2005).

Smaller firms are far behind larger firms in implementing protection measures or security controls because they lack financial and technical resources (Cragg *et al.*, 2011; Lábodi & Michelberger, 2010; Lee & Larsen, 2009). First, because of this lack of financial resources, it is difficult for SMEs to recruit and retain internal ICT[1] specialists (Cragg *et al.*, 2011; Kim *et al.*, 2017; Pritchard, 2010).

Second, SME CEOs are often alone and lack the necessary skills to identify and implement measures to mitigate IS security risks (Njenga & Jordaan, 2016). A frequent solution is to outsource their ISS to external companies or consultants (Bhattacharya, 2011; Njenga & Jordaan, 2016). SME CEOs can also rely on cloud-based solutions for their backup or SaaS-based IS security software (Kim *et al.*, 2017). However, (1) their access to external skills is often again limited by insufficient financial resources (Kim *et al.*, 2017), and (2) these outsourcing facilities mainly address technical problems and are insufficient for addressing the socio-organizational aspects of ISS such as user compliance, which is of utmost importance and increases the effectiveness of non-technical security measures (Barton *et al.*, 2016).

Consequently, SME CEOs are the sole decision-makers in most cases, and specifically with regard to strategic decisions, they play a central role in choosing and implementing ISS-related measures and controls. However, SME CEOs are not sufficiently aware of ISS issues (Njenga & Jordaan, 2016), and they consider information security to be a "large business" concern (Rees, 2010, p. 18). The ISS frameworks, methods and standards such as ISO 27002 are also considered by SME CEOs to be too complex

[1] Information & Communication Technologies.

and to be mainly tailored for large companies, leaving SME CEOs without proper guidance (Mijnhardt *et al.*, 2016).

The result is that SME CEOs often must arbitrate between the (perceived) risk level that they decide to assume and the cost of the measures that they decide to implement (Anderson & Choobineh, 2008; Dutta & McCrohan, 2002; Taylor & Brice, 2012). Therefore, the implementation of information security measures in SMEs is often intuitive (Jones, 2003) and tinkered with (Ciborra, 2002; Pritchard, 2010). Recent studies have shown that SME CEOs have a strong impact on their company's ISS (Barlette, 2008, 2012; Barton *et al.*, 2016; Lábodi & Michelberger, 2010). Consequently, investments are often poorly aligned with strategy, information is incorrectly secured, and SME CEOs may implement inadequate technical and organizational measures to protect their companies (Kayworth & Whitten, 2010; Rainer *et al.*, 2007). They can even make blatantly wrong decisions that lead to an increase in information security risks (Njenga & Jordaan, 2016). The ultimate consequence is that poorly adapted ISS can cause growth problems for SMEs because decision-making is based on inadequate information (Johnston & Hale, 2009; Perks, 2010; Raymond & Magnenat-Thalmann, 1982).

CEOs sometimes give up on ISS management because they lack IS knowledge (Rainer *et al.*, 2007), which increases the risk of severe security failures (Ross & Weill, 2002; Williams, 2007). Recent research has shown that SME CEOs are often influenced by their personal or professional network in implementing ISS protection measures (Barlette & Jaouen, 2014). These researchers have shown that such measures are often reactive, incremental and insufficient. Barton *et al.* (2016) also highlighted the importance of external influences such as the impact of mimetic mechanisms on the ISS security beliefs of senior management.

This literature review has highlighted the strategic importance of SME CEOs in addressing information security issues. In this context, it is fundamental to understand what motivates SME CEOs to protect their company information. For that purpose, the protection motivation theory is regularly used to understand the determinants of protective behaviors, notably in the social science and information security literature (see Table 1 and Appendix A).

2.2. The Protection Motivation Theory and its Applications in ISS

As a framework, we adopted the core protection motivation theory (Boss *et al.*, 2015), which is composed of a threat appraisal and a coping appraisal, enriched by social influence.

2.2.1. The protection motivation theory: origins and constructs

The protection motivation theory (PMT) was developed by Rogers (1975) based on the assumption that changes in attitudes can be triggered by fear appeals. Its purpose was to eliminate response patterns that might produce noxious consequences or to establish response patterns that might prevent the occurrence of noxious events. The original theory considered the following concepts: the *severity* of the noxious events, the *perceived vulnerability* to the threat (e.g., the probability of its occurrence), the concern about the threat and the *availability and effectiveness* of a coping response that might reduce or eliminate the potential noxious event. According to Rogers, these components lead to an intention to adopt recommended responses or not. In 1983, Rogers revised his theory by relativizing the impact of fear appeals, advocating first

that research had never found a direct relationship between emotional responses and attitude changes and second that the effective content stimuli that produce changes in attitudes had never been firmly established (Maddux & Rogers, 1983; Rogers, 1983). According to Rogers (1983, p. 158), "*attitude change is not mediated by, or a result of, an emotional state of fear*" but depends on the amount of protective motivation aroused by "*the cognitive appraisal processes of a depicted event as noxious and likely to occur, together with the belief that a recommended coping response can effectively prevent the threatened event from occurring.*"

The sources of information initiating the cognitive appraisal processes can be environmental (e.g., verbal persuasion such as fear appeals or observations of what happens to others) or intrapersonal (e.g., prior experiences with similar threats, including feedback from coping activities). These sources of information initiate two appraisal processes that determine individuals' intentions to engage in a protective behavior (Maddux & Rogers, 1983; Sommestad *et al.*, 2015): threat appraisal and coping appraisal.

Threat Appraisal. The first cognitive process is the perception of a threat. It is defined as the anticipation of a psychological, sociological or physical violation or harm to oneself or others (Workman *et al.*, 2008). People perceiving this threat will adjust their behavior according to the amount of risk they are willing to accept. The threat appraisal process triggers a behavioral adjustment based on two factors (Rogers, 1983) that decrease the probability of occurrence of a maladaptive response, that is, undesired behavior intended only to decrease fear (denying the threat, for example). The first factor is the "*severity*" of the threat, which can refer to bodily harm but can also involve intrapersonal threats such as self-esteem or interpersonal threats such as work relationships. The second factor is the "*vulnerability*" (i.e., probability) of being exposed to the threat (Rogers, 1983). The threat appraisal process leads to an adaptive response, i.e., protection motivation, which is complemented by the coping appraisal process.

Coping Appraisal. The coping appraisal process evaluates one's ability to cope with and avert the threatened danger. Coping behavior will depend on the control perceived by people with regard to a necessary behavior, their perceived capabilities, and the effort they will expend to accomplish that behavior (Bandura, 1977). Three components influence this coping appraisal: response efficacy, self-efficacy and response cost.

– *Response efficacy* corresponds to the underlying belief that the recommended coping response is effective and that the behavior engaged in by the individual is perceived to be beneficial (Rogers, 1983). Response efficacy has been demonstrated to have a main effect on intentions to protect oneself, to protect others, and on declared behavior. Response efficacy is effective if combined with the probability of the threat's occurrence. However, if the response is ineffective, an increasing probability of the threat's occurrence decreases the intentions to adopt the response. Therefore, in certain situations, an insufficient level of response efficacy may dramatically reduce the effect of fear appeals.

– *Self-efficacy* is defined as "*people's beliefs about their capabilities to produce designated levels of performance that exercise influence over events that affect their lives*" (Bandura, 1994, p. 81). In addition to relativizing the impact of "fear appeal" vs. "protection motivation," *self-efficacy* was the major new component of Roger's revised theory from 1983. Self-efficacy corresponds to the perception that one can successfully perform the coping response;

it determines whether a coping behavior will be initiated, which behavior(s) will be chosen and how much effort will be expended (Bandura, 1977; Rogers, 1983). Rogers (1983) and Maddux and Rogers (1983) identified that self-efficacy had a significantly positive effect on intention to practice protective behaviors in numerous PMT-related studies. Moreover, numerous experiments have highlighted the fact that when response efficacy or self-efficacy is high, increments in severity or vulnerability will have a simple main effect on intentions. Conversely, when response efficacy (or self-efficacy) is low, increments in severity or vulnerability will have no effect or a boomerang effect, actually reducing intentions to comply with the recommendations (Rogers, 1983).

– *Response cost* was also added by Rogers in his revised PMT. This cost corresponds to the inconvenience, expense, unpleasantness, difficulty, complexity, and side effects of overcoming the strength of habit associated with performing an adaptive response.

The perceived response efficacy and self-efficacy must outweigh the response cost to trigger a coping response.

Adding social influence to the PMT

Other variables, such as social influence, subjective norms and normative beliefs, have often been successfully used to enrich PMT results (Anderson & Agarwal, 2010; Herath & Rao, 2009; Ifinedo, 2012; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Siponen *et al.*, 2014).

Several studies of small businesses have shown that CEOs often use social and professional networks to make decisions, and such social influences may constitute a relevant variable to explain CEO behaviors (Dagorn & Poussing, 2012; Ozgen & Baron, 2007; Schoonjans *et al.*, 2013). Social influence (Ajzen, 1991) can be considered to be equivalent to subjective norms (see Venkatesh *et al.*, 2003), as it refers to the "*perceived social pressure from people who are important to someone. It corresponds to 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).

Since its creation, the PMT has been widely used in ISS research (see appendix B), mainly to study the ISS-related behaviors of employees, faculty members and students (see Table 1). In the next sub-section, we propose applying the core protection motivation theory as a framework for studying CEOs' ISS-related behaviors.

2.2.2. Application of the PMT to information security

Research on information security has examined two types of behavior: IT-related behavior consisting of the *adoption and use of protective technologies* (e.g., adoption, use or updating of anti-malware, performing backups, changing passwords) and more general *behavior related to information security* (e.g., compliance with information security policies, creating security procedures, top management support).

Until 2008, studies mainly focused on IT-related behaviors (Dinev & Hu, 2007), while after that date, approaches such as the PMT were derived based on their primary uses (e.g., clinical psychology) in the area of ISS-related behaviors (Boss *et al.*, 2015).

Studies on users' awareness-raising (Tsohou *et al.*, 2012) or developing healthy ISS behavior with the aim of developing positive behavior are mainly based on the PMT and its spinoffs (Boss *et al.*, 2015; Crossler *et al.*, 2014; Siponen *et al.*, 2014): technology threat avoidance theory (TTAT) (Liang & Xue, 2010), fear appeals (Johnston

& Warkentin, 2010) and the health belief model (HBM) (Ng *et al.*, 2009). These approaches are often enriched by researchers with other variables, such as social influence, subjective norms, normative beliefs, or moral obligation (Anderson & Agarwal, 2010).

As SME CEOs are not specialists in IT, we consider that they will mainly adopt general behavior in ISS, and therefore the PMT is better suited to explaining their behavior. The PMT has been found to be one of the most powerful explanatory theories for predicting an individual's intention to engage in protective behaviors (Anderson & Agarwal, 2010). Empirical research on the PMT has focused on the decision-making process and especially on the relationship between a potential threat and coping mechanisms when considering outcomes (Crossler *et al.*, 2014). The outcomes can be classified as "*behavioral intention*" (BI) and "*actual behavior*" (AB). Even if for Rogers (1983) BI and AB are highly overlapping, researchers today agree that they have to be distinguished. In this sense, BI corresponds to "*a person's readiness to perform a given behavior*" (Lee & Larsen, 2009, p. 179), while actual behavior or actions can be defined as "*activities or substantive personal interventions in the management of IS*" and their personal "*investment of some of their time and energy*" (Jarvenpaa & Ives, 1991, p. 206). Boss *et al.* (2015) reported that some PMT-based studies do not correctly use the core constructs of the PMT, and some even deviate dramatically from the PMT (Anderson & Agarwal, 2010; Herath & Rao, 2009; Johnston *et al.*, 2015; Tu *et al.*, 2015; Yoon & Kim, 2013). These studies can be viewed in Appendix A.

The initial formulation of the PMT in social and clinical psychology used BI as the dependent variable (Crossler *et al.,* 2014), and research on information security has often adopted a similar perspective by measuring an individual's behavioral intention. However, recent PMT studies focused on AB rather than BI as the dependent variable (Neuwirth *et al.*, 2000; Woon *et al.*, 2005). Researchers considered that actual behavior is the true phenomenon of interest (Crossler *et al.*, 2014) because the ultimate goal is to change security behaviors, not just intention (Boss *et al.*, 2015, p. 859). Furthermore, Limayem *et al.* (2007) advised scholars to include AB in their studies, as they advocated that including AB prevented researchers from reaching the wrong conclusions.

Table 1 summarizes the relevant literature by identifying nine studies that use the core PMT variables as advocated by Boss *et al.* (2015). A detailed table including the constructs used is provided in Appendix B.

In Table 1, we observe that four studies addressed general behavior such as complying with an ISS policy (Crossler & Bélanger, 2014; Ifinedo, 2012; Siponen *et al.*, 2014; Vance *et al.*, 2012), four addressed a specific technology/software use or adoption such as anti-spyware or anti-malware (Johnston & Warkentin, 2010; Liang & Xue, 2010), backup (Boss *et al.*, 2015), and anti-plagiarism (Lee, 2011), and one addressed the intention to support and encourage behavior with regard to the purchase of anti-malware software (Lee & Larsen, 2009). We can observe that five studies out of nine used BI and AB as dependent variables.

Furthermore, we can also observe that four studies included, at least partially, students in their sample: even though these studies may provide rich insights because they used elaborate experimentations, students may not reflect actual behavior in a professional context or in work settings (Anderson & Agarwal, 2010, p. 620). None of these studies focused on SME CEOs.

Papers	Year	Target & Firm Size	Behavioral Intention	Actual Behavior
Lee & Larsen	2009	SME Executives	Support, encourage purchase	Purchases of anti-malware software
Johnston & Warkentin	2010	Faculty, Staff & Students	Use of anti-spyware	N/A
Liang & Xue	2010	Students	Use of anti-spyware	Use & updating of anti-spyware
Lee	2011	Faculty	Intention to adopt an anti-plagiarism system	Anti-plagiarism system adoption
Ifinedo	2012	Employees All Sizes	Compliance with Orga ISSP	N/A
Vance *et al.*	2012	Administrative City Govt	Compliance with Orga ISSP	N/A
Crossler & Bélanger	2014	Students	N/A	Security practices
Siponen *et al.*	2014	Employees All Sizes (2006)[2]	Compliance with Orga ISSP	Compliance with Orga ISSP + recommend & assist
Boss *et al.*	2015	Students	(1) Make backup (2) Use anti-malware	(1) Make backup (2) Use anti-malware

ISSP: IS Security Policy.

Table 1. Previous studies using the core PMT and their characteristics

Our literature review showed that SME CEOs seem to engage in specific ISS behaviors and that the PMT constitutes a relevant framework to explain their protective behavior. In fact, Table 1 shows that using the PMT, only Lee and Larsen (2009) studied ISS in SMEs, but the authors did not distinguish between CEOs and other executives (CIOs, CFOs, etc.). Thus, to better understand SME CEO's ISS behavior, in this study, we question the antecedents of the protection intention and actual behavior of SME CEOs using the PMT framework.

3. RESEARCH MODEL AND HYPOTHESES

This study adopts the protection motivation theory and develops a theoretical model to address CEOs' behavioral intention and actual behavior regarding the implementation of information security

[2] Date of the survey (8 years).

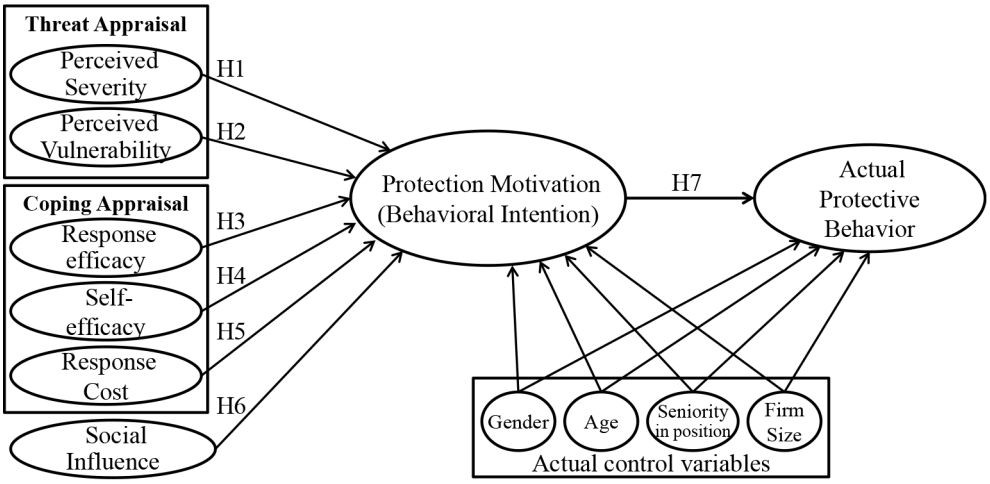

Figure 1. Research Model

measures (see Figure 1). The hypotheses in our theoretical model therefore indicate that (1) the intention to implement information security measures is a positive linear function of four constructs: (a) perceived severity of the threat, (b) perceived vulnerability to the threat, (c) response efficacy, and (d) self-efficacy; and (2) intention is a negative linear function of the response cost. This study extends the theoretical boundary of the PMT by investigating the impact of social influence on behavioral intention.

The PMT divides the variables that influence behavior/intention into two categories: threat appraisal variables and coping appraisal variables. Threat appraisal comprises perceived vulnerability and perceived severity, while coping appraisal includes three dimensions: response efficacy, self-efficacy and response cost. We have defined these dimensions in the previous section. Based on previous research on information security and studies using the PMT (see Table 1), we developed the following hypotheses.

Threat appraisal is associated with threats or dangers from continuous maladaptive responses (Lee & Larsen, 2009). An increase in perceived severity and vulnerability leads to greater behavioral intention in a healthier manner. It encompasses perceived severity and perceived vulnerability.

Perceived severity corresponds to the perception of the severity of the consequences, e.g., "*the level of the potential impact*" (Vance *et al.*, 2012, p. 192), of an ISS problem because previous ISS measures were insufficient or ineffective (Ifinedo, 2012; Liang & Xue, 2010). It includes, for example, the perceived level of a company's loss of activity, loss of data, financial losses and the potential side effects (e.g., loss of image). This perceived severity will lead people to behave in a more cautious manner if this perception increases, but the reverse effect also exists, i.e., people will be less cautious if the perceived severity diminishes (Bulgurcu *et al.*, 2010; Herath & Rao, 2009). As SME CEOs may not generally have technical skills, we postulate as follows:

- *H1: The perceived severity of potential information security threats positively and significantly influences SME CEOs'*

protection motivation to implement information security-related measures.

Perceived vulnerability is the conditional probability that a threatening event will occur provided that no adaptive behavior is performed or there is no adaptation of an existing behavior (Lee & Larsen, 2009). The greater the perceived vulnerability there is to a security breach, the more ISS behaviors people will engage in (Ryan, 2004), and the opposite can also be true, i.e., perceived invulnerability can lead to fewer ISS behaviors (Bulgurcu *et al.*, 2010; Ryan, 2004).

We postulate as follows:

• *H2: The perceived vulnerability from potential information security threats positively and significantly influences SME CEOs' protection motivation to implement information security-related measures.*

Coping appraisal corresponds to a respondent's ability to respond to a threat. It encompasses response efficacy, self-efficacy and response cost.

Response efficacy, in the context of our research, refers to CEOs' beliefs about whether implementing information security-related measures can enhance their company's security and reduce security flaws. If people perceive the available coping mechanisms to be adequate, for example, because the available security measures are improving (Kankanhalli *et al.*, 2003), they are more likely to engage in an ISS-related behavior. On the contrary, if people have a negative perception of the efficacy of a necessary behavior because no matter what they do, security breaches will continue to increase, they will be more likely to omit this behavior (Workman *et al.*, 2008).

Therefore, we postulate as follows:

• *H3: The response efficacy to potential information security threats positively and significantly influences SME CEOs' protection motivation to implement information security-related measures.*

Self-efficacy refers to CEOs' belief in their own ability to implement information security-related measures. Prior research has demonstrated that people are more motivated to cope with or perform ISS security behaviors as the level of their self-efficacy increases (Workman *et al.*, 2008). In the field of information security, all but one out of the nine studies using the core PMT variables (see Appendix B) found self-efficacy to have a significantly positive effect on behavioral intention. Hence, we postulate as follows:

• *H4: Self-efficacy to potential information security threats positively and significantly influences SME CEOs' protection motivation to implement information security-related measures.*

Response cost refers to the physical and cognitive efforts necessary for an adaptive response (Liang & Xue, 2010). It can correspond to the money or time required to invest in the behavior or security measure or the inconvenience or difficulty of the behavior itself. This perceived effort is balanced by the perceived value of the ISS-related behavior (Workman *et al.*, 2008). The response cost represents any costs (e.g., time, monetary, difficulty, complexity, effort) associated with taking the adaptive coping response.

We therefore postulate as follows:

• *H5: The response cost negatively influences SME CEOs' protection motivation to implement information security-related measures.*

Social influence has been operationalized in the PMT as the influence of customers, partners and competitors (see Appendix D). It has proved to be significant in many studies addressing information security. In the eighteen studies using the "core" or "non-core" PMT (see Appendix B),

Variable Name	Previous Core PMT Studies	Identified / Expected Effect
Gender	Boss *et al.*, 2015; Ifinedo, 2012; Johnston & Warkentin, 2010; Lee, 2011; Liang & Xue, 2010; Siponen *et al.,* 2014; Vance *et al.*, 2012.	For men, a greater impact was found on behavioral intention by Herath and Rao (*) (2009) and on actual behavior by Lee (2011).
Age	Boss *et al.*, 2015; Crossler & Bélanger, 2014; Ifinedo, 2012; Johnston & Warkentin, 2010; Lee, 2011; Liang & Xue, 2010.	A negative impact on behavioral intention was identified by Anderson and Agarwal (*) (2010) and Boss *et al.* (2015).
Seniority in position	Boss *et al.*, 2015; Crossler & Bélanger, 2014; Johnston & Warkentin, 2010; Lee, 2011; Siponen *et al.,* 2014.	A positive impact on actual behavior was identified by Boss *et al.* (2015) and Crossler *et al.* (*) (2014).
Firm size	Ifinedo, 2012; Lee & Larsen, 2009.	Hypothesized a positive influence on actual behavior (Lee & Larsen, 2009). No actual impact was found in any previous PMT studies.

(*) Non-core PMT study.

Table 2. Control variables and their expected effects

social influence or similar variables such as subjective norms and normative beliefs have been introduced nine times. Its effects were mainly significant and often had a stronger effect on the motivation to undertake protective behaviors (Herath & Rao, 2009; Johnston & Warkentin, 2010; Siponen *et al.*, 2014; Tu *et al.*, 2015). We therefore postulate as follows:

- *H6: Social influence has a positive and significant impact on SME CEOs' protection motivation to perform information security-related measures.*

Behavioral intention, or protection motivation, indicates a person's readiness to perform a given behavior (Lee & Larsen, 2009). *Actual behavior* is the action realized to protect an information system. The significant relationship between behavioral intention and actual behavior has been demonstrated in several studies (Boss *et al.*, 2015; Crossler *et al.*, 2014; Delone & McLean, 2003; Lee & Larsen, 2009; Siponen *et al.*, 2014). Over the nine core PMT studies, eight of them analyzed behavioral intention, and five found a positive link with actual behavior (Boss *et al.*, 2015; Lee, 2011; Lee & Larsen, 2009; Liang & Xue, 2010; Siponen *et al.*, 2014). As for previous studies, we predict that when SME CEOs intend to protect their information, they are more inclined to actually implement security measures. Consequently, we postulate as follows:

- *H7: Behavioral intention has a positive and significant impact on SME CEOs' actual behavior to perform information security-related measures.*

We used the most common control variables employed in literature (see Appendix C). Table 2 shows the control variables that we included in our study in descending frequency of use in previous studies.

4. METHODOLOGY

4.1. Research design

The research model was tested using a field survey. We used a random sample of 9500 French SMEs that were accessed through Kompass and alumni databases. Each participant received an email explaining the purpose of our study, including a link to our web-based questionnaire. A total of 374 responses were returned between December 2014 and April 2015. After removing incomplete and invalid responses, we obtained 292 usable responses. Response rates for information security-related surveys are usually low (Kotulic & Clark, 2004). In addition, SME CEOs are very difficult to contact by email, and time is a scarce resource for them (Wolcott *et al.*, 2008).

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

– The response efficacy scale (REFF) used measures adapted from Vance *et al.* (2012) and Ifinedo (2012). The self-efficacy scale (SEFF) used measures borrowed from Lent *et al.* (2006), Vance *et al.* (2012) and Ifinedo (2012). The response cost measure (COST) was adapted from Vance *et al.* (2012).

– The perceived severity scale (SEV) used measures adapted from Vance *et al.* (2012) and Siponen *et al.* (2014). The perceived vulnerability scale (VULN) used measures borrowed from Vance *et al.* (2012), Ifinedo (2012) and Siponen *et al.* (2014).

– For social influence (SINFL), we adapted the scales developed by Ho (2000), Lee and Larsen (2009) and Anderson and Agarwal (2010).

– Behavioral intention to implement security measures (BI) and actual related behavior (AB_Gen) used scales adapted from Workman *et al.* (2008) and Yoon and Kim (2013).

The questions included in our instrument were first pre-tested through face-to-face interviews with SME CEOs (N=14). Based on the CEOs' feedback, the readability of the questions was improved through several rounds. The questionnaire itself was created using the Qualtrics tool. At the beginning of the questionnaire, an introductory section defined information security, offered examples of possible actions, and specified that only CEOs of businesses with less than 250 employees were authorized to respond. Participation in the study was voluntary, and respondents were assured that individual responses would be treated with anonymity and confidentiality.

4.2. Measures

Our purpose was to determine the influence of the PMT variables and social influence on behavioral intention and actual behavior with regard to the implementation of information security measures. We detail all the variables and items in our questionnaire in Appendix D. All items were measured using 7-point Likert scales anchored at 1="Strongly disagree" and 7="Strongly agree". In order to perform the multi-group analysis, the ownership (OWNER) of the company was included in the form of a dummy variable (non-owner = 0; owner = 1).

Concerning the control variables, we included gender (GENDER) in the form of a dummy variable (male = 0; female = 1). Firm size (SIZE) was measured using the number of employees (between 0, i.e., entrepreneur alone, and 250). Seniority in position (SENIOR) corresponds to the number of years in the position of CEO,

and Age (AGE) represents the respondent's age.

5. DATA ANALYSIS AND RESULTS

To validate the measurements and test our hypotheses, we used Partial Least Squares (PLS-SEM) analyses. PLS places minimal demands on sample size, measurement scales and residual distributions (Chin, 1998; Gefen *et al.*, 2000). PLS is also best suited for testing complex structural models, as it avoids inadmissible solutions and factor indeterminacy (Fornell & Bookstein, 1982).

5.1. Descriptive statistics

As shown in Table 3, the majority of the respondents were male (76%). Our proportion of 24% of female CEOs is close to the European figure of 29% (European Union, 2014). The sizes of the companies were distributed as follows: 59% micro-firms with less than ten employees, 30% businesses with between 10 and 49 employees, and 11% medium-sized businesses (see Table 3). Our sample shows a slight over-representation of the smallest businesses compared to European figures (OECD, 2013) but is closer to that of previous studies dedicated to information security in SMEs (Gupta & Hammond, 2005; Lee & Larsen, 2009). The average firm size was 25.4 employees, and the average age was 40.4 years old.

Variable	Frequency	Percent
Gender		
Male	223	76.4%
Female	69	23.6%
Firm Size		
0-9	172	59%
10-49	88	30%
50-250	32	11%

Table 3. Demographic characteristics of the sample (N=292)

5.2. Model assessment

Overall fit

Bootstrapping allows us to obtain the model fit, i.e., to identify the likelihood of a potential discrepancy between the empirical and the model-implied correlation matrix. This discrepancy can be assessed though two indicators: the geodesic discrepancy (dG) and the unweighted least squares discrepancy (dULS) (Dijkstra & Henseler, 2015). Our bootstrapping test was performed on 5000 iterations, as advised by Hair *et al*. (2017). Following Henseler *et al*.'s (2016) guidelines, we provide in Table 4 the results for both the estimated and saturated[3] models.

Based on the thresholds provided by Henseler *et al.* (2016), dULS and dG (Values) are far below their respective 95% bootstrap

	Value (saturated)	HI95 (saturated)	Value (estimated)	HI95 (estimated)
dULS	0.898	11.230	1.270	11.022
dG	0.510	3.429	0.549	3.592

Table 4. Model fit assessment: geodesic and unweighted least squares discrepancies

[3] In the saturated models, all constructs correlate freely.

Latent Variable	Cronbach's α	Jöreskog's Rho	AVE	SEV	VULN	REFF	SEFF	COST	SINFL	BI
SEV	0.796	0.880	0.700	**0.837**						
VULN	0.854	0.912	0.774	0.500	**0.880**					
REFF	0.853	0.932	0.872	0.327	0.366	**0.934**				
SEFF	0.876	0.924	0.800	0.089	0.164	0.348	**0.894**			
COST	0.767	0.866	0.663	0.089	0.032	0.032	0.071	**0.814**		
SINFL	0.826	0.897	0.744	0.315	0.319	0.255	0.095	0.205	**0.863**	
BI	0.890	0.948	0.901	0.161	0.247	0.349	0.253	0.217	0.367	**0.949**

Table 5. Inter-construct correlations and squared root of AVE along the diagonal

quantile (HI95) in both the estimated and saturated models. Hence, in proportion with the 95% bootstrap quantile (HI95), the discrepancy values for our estimated model are very close to those of the corresponding saturated model, indicating a good fit. Therefore, we can conclude that the overall fit of our model is satisfactory, i.e., the discrepancy between the empirical and the model-implied correlation matrix is not significant.

Measurement model analysis

Table 5 shows the values resulting from our measurement model analysis.

Indicator reliability and constructs' internal consistency reliability

Indicator reliability and the constructs' internal consistency reliability can be assessed by applying the following criteria: (1) all Cronbach's α values exceed 0.7, and (2) all Jöreskog's Rho values (Jöreskog, 1971) are within the interval [0.7-0.95], indicating that they meet the "satisfactory to good" condition (Hair *et al.*, 2017)[4]. All AVE (average variance extracted) values are over 0.5, indicating good convergent validity of the constructs. This result means that each construct explains more than 50% of the variance of its indicators (Hair et al., 2011).

Discriminant validity

Discriminant validity was assessed through two criteria: (1) the Fornell-Larcker criterion is met in Table 5 because for each construct, the squared root of the AVE (in bold) exceeds the highest correlation with other constructs (Fornell & Larcker, 1981), and (2) in Table 6, the indicator's outer loadings on the construct they are intended to measure exhibited higher loadings than the cross-loadings with other constructs (Hair *et al.*, 2017).

Structural model analysis

We first analyzed the model's predictive accuracy and then the structural model relationships.

The model's predictive accuracy can be assessed using R^2 (see Table 7).

Our R^2 values are close to those of the adjusted and "bootstrapped" R^2 (less than 3%), T is higher than 2.57 (1% probability of error), and 0 does not fall within the calculated interval, indicating satisfactory

[4] Values over 0.95 are considered to be "problematic," as the items are almost redundant (Drolet & Morrison, 2001).

	SEV	VULN	REFF	SEFF	COST	SINFL	BI
SEV1	**0,826**	0,453	0,237	0,038	0,065	0,290	0,123
SEV2	**0,910**	0,457	0,318	0,102	0,096	0,287	0,175
SEV3	**0,768**	0,318	0,257	0,070	0,059	0,191	0,076
VULN1	0,444	**0,895**	0,370	0,174	-0,036	0,228	0,230
VULN2	0,391	**0,895**	0,337	0,169	-0,015	0,302	0,222
VULN3	0,493	**0,849**	0,252	0,082	-0,019	0,319	0,200
REFF1	0,331	0,383	**0,937**	0,354	-0,036	0,196	0,333
REFF2	0,279	0,299	**0,931**	0,296	-0,014	0,282	0,320
SEFF1	0,074	0,081	0,309	**0,844**	-0,009	0,042	0,195
SEFF2	0,086	0,183	0,340	**0,926**	-0,137	0,113	0,208
SEFF3	0,076	0,167	0,293	**0,912**	-0,039	0,094	0,266
COST1	0,154	0,097	-0,049	-0,059	**0,846**	0,201	0,205
COST2	0,005	-0,144	-0,119	-0,040	**0,740**	0,030	0,068
COST3	0,020	-0,104	0,037	-0,060	**0,851**	0,186	0,196
INFL1	0,267	0,339	0,239	0,134	0,059	**0,763**	0,258
INFL2	0,283	0,230	0,213	0,058	0,239	**0,914**	0,332
INFL3	0,268	0,275	0,216	0,066	0,205	**0,901**	0,352
BI1	0,161	0,232	0,353	0,228	0,218	0,371	**0,950**
BI2	0,145	0,238	0,311	0,253	0,194	0,327	**0,949**

Table 6. Loadings and cross-loadings

	R^2	R^2 (adj)	R^2 (bootstrap)	T	Interval (95%)	
Behavioral Intention (BI)	**0.277**	0.254	0.306	6.453	0.226	0.393
Actual Behavior (AB)	**0.143**	0.131	0.159	3.584	0.089	0.242

Table 7. R^2 for dependent variables

Latent variable	**Path coefficient**	**t-value**	**p-value**	**Significance**
Severity (SEV)	-0.07	-1.107	0.269	
Vulnerability (VULN)	0.10	1.585	0.114	
Response Efficacy (REFF)	0.23	3.742	0.000	***
Self-Efficacy (SEFF)	0.15	2.659	0.008	**
Response Cost (COST)	0.19	3.561	0.000	***
Social Influence (SINFL)	0.24	4.261	0.000	***
Gender	-0.04	-0.843	0.400	
Age	0.05	0.718	0.474	
Seniority in position	-0.12	-1.776	0.077	
Firm size	0.06	1.100	0.272	

Table 8. Tests of hypotheses and control variables on behavioral intention (BI)

Latent variable	Path coefficient	t-value	p-value	Significance
Behavioral Intention (BI)	0.32	5.809	0.000	***
Gender	-0.11	-2.052	0.041	*
Age	0.02	0.246	0.806	
Seniority in position	0.09	1.250	0.212	
Firm size	-0.11	-2.041	0.042	*

Table 9. Tests of hypotheses and control variables on actual behavior (AB)

quality and stability of our results. The bootstrapping test provided the estimates of standard errors for testing the statistical significance of the path coefficients using t-tests (Tables 8 and 9).

Except for perceived severity and perceived vulnerability, all variables showed a significant influence on protection motivation. However, response cost exhibited the opposite of the expected effect. None of the control variables showed any significant effect.

Behavioral intention exerts a strong and significant influence on SME CEOs' actual behavior. Gender and size exert a small and negative influence on actual behavior. Figure 2 shows our results for the full sample.

Common method bias assessment

Because our survey data were self-reported and can potentially be confounded by common method bias (Podsakoff *et al.*, 2003), and because we only had an assessment of the reported behavior and

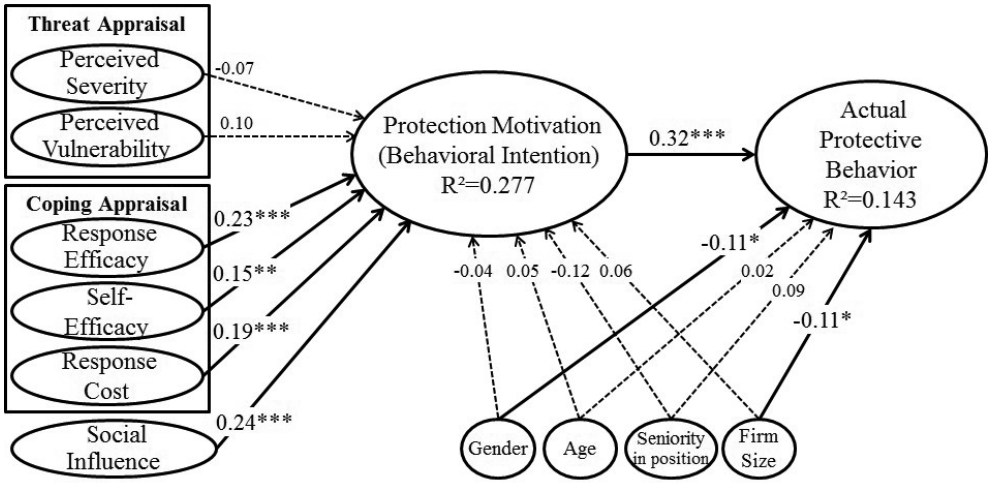

Figure 2. Full sample results (N=292)

not actually measured behavior (Straub *et al.*, 1995), we used several means to assess and minimize the potential common method bias.

First, after data collection, we conducted Harman's single factor test (Podsakoff *et al.*, 2003) to control for single-respondent bias. The largest covariance among all the constructs explained by one factor in our data is 35.7%, which is well below the 50% rule-of-thumb cut-off (Podsakoff & Organ, 1986).

Second, we used the approach described by Liang *et al.* (2007). We included in our PLS model a latent method factor: for the detailed results and approach, see Appendix E. These results demonstrate that the average substantively explained variance of the indicators ($R1^2$) is 0.77, while the average method-based variance ($R2^2$) is 0.003. $R1^2$ largely exceeds $R2^2$ (the ratio is 277:1), and most method factor loadings are not significant.

Third, we performed several crosschecks to increase the reliability of our questionnaire, and fourth, the results of our structural model demonstrated different levels of significance for the path coefficients.

For these reasons, we can assume that CMV bias is unlikely to be a serious concern in our study.

5.3. Multi-group analysis

According to Hair *et al.*'s (2017) guidelines, the minimum sample size should be greater than 10 times the largest number of structural paths directed at a particular construct in the structural model. As the number of paths directed at Behavioral Intention (BI) is 10, our sample should exceed 100 observations. The literature review showed that SME CEOs engage in specific behaviors in terms of IS implementation, management and protection in comparison to large firm executives, students or employees. Moreover, it has been shown that owner and non-owner CEOs may engage in different behaviors. In order to test these differences, we conducted a multi-group analysis by dividing the subjects according to the ownership of the SME. Using this binary item, we classified each CEO as an owner (n=183) or a non-owner (n=109), and both subgroups met Hair *et al.*'s (2017) guidelines for the minimum sample size.

To assess the significance and relevance of this multi-group analysis, we performed multi-group tests (see Appendix F). They confirm that the difference between owners and non-owners is significant. In addition, permutation tests exhibited significant differences between the two groups for perceived vulnerability on BI, self-efficacy on BI and the influence of BI on actual protective behavior (see Appendix F). As our measurement model has previously been validated, we only present the results for the path analysis in Figures 3 and 4. They reveal several interesting differences between the two groups.

In Figure 3, we observe that non-owner CEOs' behavior is in line with previous core PMT studies (see Appendix B). These results are very consistent with Lee and Larsen's study (2009), which is the only one addressing executives in SMEs, especially if we compare the non-owner subgroup with their non-IT-skilled executive subgroup: Coping appraisal is the main reason that drives non-owner CEOs to intend to implement information security measures, while threat appraisal and social influence are much less significant. Conversely, SME owners exhibited significantly different behaviors, as shown in Figure 4.

We can observe that the effects of the independent variables in Figure 4 are almost

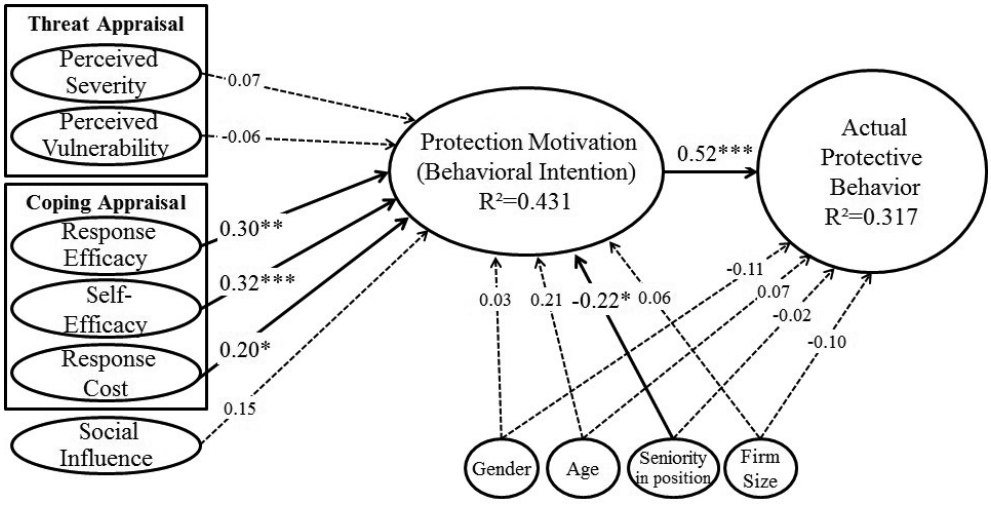

Figure 3. Results for non-owner CEOs (n=109)

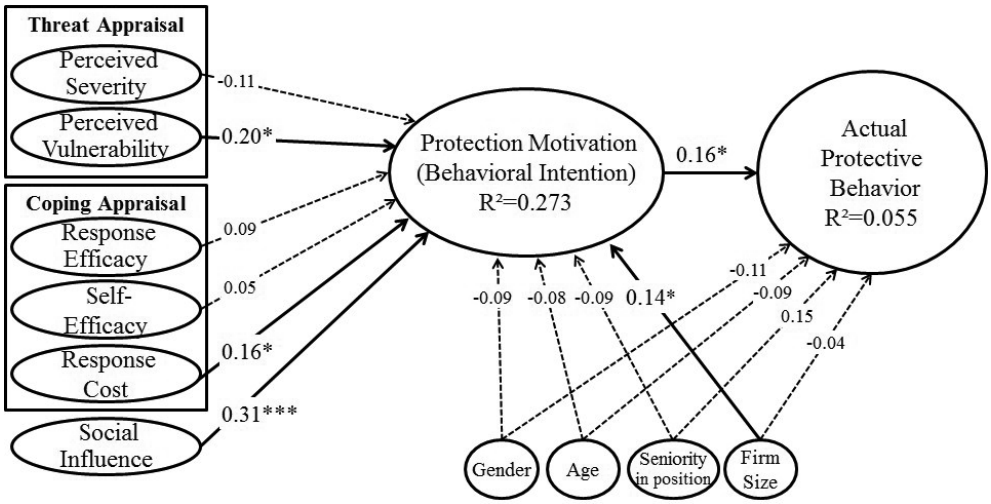

Figure 4. Results for owner CEOs (n=183)

completely different when compared with Figure 3:

• Except for *perceived severity* and *response cost*, which exhibit comparable effects, the variables that were significant become non-significant and vice-versa. *Perceived vulnerability* and *social influence* become significant, while *response efficacy* and *self-efficacy* become non-significant.

• The R squared for protection motivation decreases from 0.431 to 0.273.

• The magnitude of the link between BI and AB decreases dramatically from 0.52*** to 0.16*, i.e., more than three times less.

• The explained variance for actual protective behavior drops dramatically to almost 0 as the R squared decreases from 0.317 to 0.055, which is nearly six times less.

		General Model	Owner CEOs	Non-Owner CEOs
Threat appraisal → (BI)	Perceived Severity	-0.07	-0.11	0.07
	Perceived Vulnerability	0.10	**0.20***	0.06
Coping Appraisal → (BI)	Response Efficacy	**0.23*****	0.09	**0.30****
	Self-Efficacy	**0.15****	0.05	**0.32****
	Response-Cost	**0.19*****	**0.16***	**0.20***
Social Influence → (BI)		**0.24*****	**0.31*****	0.15
Control Variables → (BI)	Gender	-0.04	-0.09	0.03
	Age	0.05	-0.08	0.21
	Seniority in Position	-0.12	-0.09	**0.22***
	Firm Size	0.06	**0.14***	0.06
Control Variables → (AB)	Gender	**-0.11***	-0.11	-0.11
	Age	0.02	-0.09	0.07
	Seniority in Position	0.09	0.15	-0.02
	Firm Size	**-0.11***	-0.04	-0.10
Behavioral Intention (BI) → Actual Behavior (AB)		(BI: R^2=0.277) (AB: R^2=0.143) **0.32*****	(BI: R^2=0.273) (AB: R^2=0.055) **0.16***	(BI: R^2=0.431) (AB: R^2=0.317) **0.52*****

Table 10. Comparison of the results

We show that owners are significantly motivated to protect their information by the following variables: perceived vulnerability (0.20*), response cost (0.16*), social influence (0.31***) and the control variable firm size (0.14*), while non-owners are influenced by the variables response efficacy (0.30**), self-efficacy (0.32**), response cost (0.20*) and the control variable seniority (0.22*) (see Table 10).

Rogers (1983) determined that response efficacy and self-efficacy were at the root of any protective motivation, and these two factors are not significant in the case of SME owners. Moreover, social influence, which is not part of the PMT, becomes the most influential and significant variable explaining SME owners' protection motivation. However, this behavioral intention does not lead to actual protective behaviors. The next section will discuss this very interesting difference between the two populations, the magnitude of which was completely unexpected.

6. DISCUSSION

Our results emphasize some important issues regarding information security behavior in SMEs. For instance, we identified a behavioral and motivational difference between SME owners and non-owners.

	General Model (N=292)	Owner CEOs (N=183)	Non-Owner CEOs (N=109)
H1 Perceived severity ⇨ Behavioral intention	Not Supported	Not Supported	Not Supported
H2 Perceived vulnerability ⇨ Behavioral intention	Not Supported	Supported	Not Supported
H3 Response efficacy ⇨ Behavioral intention	Supported	Not Supported	Supported
H4 Self-efficacy ⇨ Behavioral intention	Supported	Not Supported	Supported
H5 Response cost ⇨ Behavioral intention	Not Supported (reverse effect)	Not Supported (reverse effect)	Not Supported (reverse effect)
H6 Social influence ⇨ Behavioral intention	Supported	Supported	Not Supported
H7 Behavioral intention ⇨ Actual behavior	Supported	Supported	Supported

Table 11. Hypotheses support for the three models

6.1. Interpretation of results

Regarding the general model based on PMT (see Table 11), our results are mainly in line with previous PMT studies (e.g., Boss *et al.*, 2015; Lee, 2011; Vance *et al.*, 2012). All hypotheses are supported, except for response cost (H5), which is sometimes not significant or not included in the studies (see appendix B); perceived vulnerability (H2), which also sometimes is non-significant or has a reverse effect (Crossler & Belanger, 2014); and perceived severity (H1), which can sometimes have a reverse effect (Ifinedo, 2012; Johnston & Warketin, 2010).

To explain this disparity of outcomes for H1 and H2, Johnston *et al.* (2015) argue that PMT was primarily developed and used to address *threats to the physical self* in healthcare contexts; hence, perceived severity and perceived vulnerability have *personal relevance*. In studies regarding the company and specifically ISS, as underlined by Johnston *et al.* (2015), *threats to the individual's things* (e.g., data, information, and systems) may be non-personally relevant. This must be nuanced for CEOs and specifically SME owners, as literature underlines that they have a propensity to assimilate themselves to their company (i.e., Courrent & Gundolf, 2009). This can explain the results of our study regarding SME owners (Model 'Owner CEOs' in Table 11), where perceived vulnerability was significant.

Nonetheless, we agree with Johnston *et al.* (2015) that the general PMT model could be amended when addressing employees' ISS-related behaviors in the context of *threats to an organization's information assets*, where perceived severity and perceived vulnerability can have limited personal relevance.

However, a deeper investigation using multi-group analysis shows an important heterogeneity, distinguishing owner from non-owner CEOs. While non-owners show consistent behaviors with other PMT-studied populations, the results for owners are significantly different. Questioning why owner CEOs have a lower tendency to protect their

companies' information than non-owner CEOs implies looking for what motivates protective behaviors in both populations.

6.1.1. Non-owner CEOs

As previously highlighted, our results concerning non-owner CEOs are very close to those of previous PMT studies. These results extend the validity of the protection motivation theory with regard to non-owner CEOs for the variables of coping appraisal but not for those of threat appraisal, which appear to be non-significant in our study[5].

Response efficacy and self-efficacy proved to have strong and significant effects (0.30** and 0.32***, respectively) on behavioral intention. This result is in line with psychological studies using the PMT (Maddux & Rogers, 1983; Rogers, 1983) that led to the conclusion that both factors are the main elements triggering protective behavior. Our results are also consistent with the majority of PMT-related studies (core and non-core PMT), as 13 studies out of 18 also highlighted such strong effects. Furthermore, our results extend those of Kankanhalli *et al.* (2003) by specifically examining CEOs and showing that when they have a positive perception of their behavioral efficacy, they intend to be more secure and to implement ISS measures. Although we show that the behavioral intention to implement information security measures has a strong and significant impact on actual behavior (0.52***) for non-owner CEOs, surprisingly, this impact becomes weak and non-significant for owner CEOs.

One recent study mobilized *agency theory* to explain SME CEOs' behaviors according the parameter "non-ownership". Gamble *et al.* (2013) observed that many entrepreneurs contract with non-owners to manage their company's operations because the entrepreneurs may have investments in a number of businesses or lack certain operating expertise. The agency problem consists of a possible divergence of interests between the owner and his/her CEO, called here the "principal" and the "agent", with the agent acting as a representative of the principal (Jensen & Meckling, 1976). Agency theory advocates that the priorities and objectives of owners (principals) and CEOs (agents) may differ based upon their divergent interests (Dalton *et al.*, 2007). To overcome these differences in goal achievement and to reduce the costs associated with them, the two parties can enter into a contract that provides incentives for the CEO to achieve the goals of the owner (Jensen & Meckling, 1976). The mission of the non-owner CEO is to obtain an efficient and sustainable business. Protection is therefore quite natural in order to preserve the firm as well as to maintain his/her own employment. As their work and income largely depend on firm performance, non-owner CEOs do not want to create uncertainties that could increase organizational and financial risks for the firm (Gamble *et al.*, 2013).

Finally, response cost is often non-significant in PMT-related studies (see Appendix B). Interestingly, in our study, it exerts a positive influence on intention to protect information (0.20*), which is a counterintuitive result that moreover exhibits a reverse effect compared with the effect found in previous studies. This result suggests that the more costly CEOs feel that their behavior is in terms of effort or inconvenience, the more important their behavioral intention will be. An explanation for this result could be the fact that they are conscious of the investment that information protection represents, thereby illustrating its

[5] None of our control variables had a significant effect, except for seniority in position (0.22*), in line with previous studies in Table 2.

necessity. We can assume that CEOs may feel that information security requires vital and compulsory changes in their businesses. Therefore, in this case, response cost could be linked with the perception of ISS as a strategic issue and with the level of CEOs' commitment to their businesses.

6.1.2. Owner CEOs

If owners and non-owners are similar with regard to the influence of response cost (0.20* and 0.16* respectively), the major difference between them is that the path coefficient between owner CEOs' behavioral intention and actual protective behavior decreases dramatically, leading to a very small explanation of owner CEOs' actual protective behavior.

Lorenz *et al.* (2015) recently compared owner and non-owner CEOs and concluded that owners were more risk-averse than non-owners. This result is consistent with several studies on the risk aversion of SME owners compared to non-owners or entrepreneurs (Stewart *et al.*, 1999; Wagener *et al.*, 2010). These findings should argue in favor of greater protective behavior when the CEO owns the company. One could suppose that owners would have greater protection motivation than non-owners, but only perceived vulnerability (0.20*) and response cost (0.16*) influence behavioral intention with regard to the core PMT model. Moreover, if owners are conscious of their vulnerability and intend to implement protection measures, this intention is relatively weakly transformed into action (0.16*).

Regarding now the enriched PMT model, the importance of the path coefficient for social influence (0.31***) highlights the necessity for further investigation of other explanatory variables. The score for social influence confirms the results of previous qualitative surveys showing that some SME owners implement security measures because their advisors (i.e., customers, partners, competitors and personal networks) do so or ask them to do so (Barlette & Jaouen, 2014).

6.2. Theoretical contributions

This study makes important contributions to the field on information security. First, it constitutes the first research to focus solely on SME CEOs' protection motivation. While our results for non-owner CEOs confirm and extend previous research on the protection motivation theory, owner CEOs' behaviors exhibit important discrepancies compared with non-owners.

Second, academic researchers have previously explored the differences between small business owners and entrepreneurs, between owners and managers, or between owners and non-owners, essentially in terms of personality traits, competences and risk-taking (Anderson *et al.*, 1990; Carland *et al.*, 1984; Gamble *et al.*, 2013; Lorenz *et al.*, 2015; Wagener *et al.*, 2010). We have found no academic study analyzing ISS (or even IS) behaviors based on ownership and comparing owners with non-owners. Consequently, we proposed theories that supplement the PMT when addressing CEOs' behavioral issues, such as agency theory, and we showed that social influence constitutes a very important construct in explaining owner CEOs' behaviors.

Last, as this important finding of a discrepancy between owner and non-owner CEOs deserves further studies, we offer a detailed list of avenues for future research to address the differences between these two populations.

For all the reasons above, we can state that this research contributes to – and shares ideas for – a better understanding of small business owners' and non-owners' information security behaviors. For future research, we advise researchers to conduct

studies explicitly differentiating owner from non-owner CEOs.

Although our findings provide meaningful implications, this study has some limitations. First, the study examined only positive actions rather than maladaptive actions: even if SME CEOs are expected to exert positive actions (in contrast to some employees), this expectation may require further investigation. Second, in addition to CEOs' ISS-related behaviors, we could have gauged the ability of an organization and its employees to act to protect information. Third, future studies should assess objective (i.e., measured) behavior, as we could only access self-reported protective behavior using our web-based questionnaire. Fourth, we could not determine the effects of certain variables, such as industry type or whether a company is IT intensive (Lee & Larsen, 2009).

6.3. Avenues for future research

This research opens several paths for future investigations. How can we address the difference between owner and non-owner CEOs, and what other variables should be considered to explain the protective behaviors of SME owners?

Considering the decrease in the PMT model's predictive power between behavioral intention and actual behavior for owners, a study of the intention-action gap could be conducted in this context. Komatsu *et al.* (2013) analyzed the misalignment between ISS-related behavioral intention and the actual behavior of individuals. They found that intention indirectly affects participants' actual behavior via cognitive elements. The variables included, for instance, perceived social dilemma, persuasiveness of message, social norms, level of involvement and responsibility. They also suggested that some PMT variables could act as moderators between intention and action. Furthermore, they proposed that intention affects these elements and, subsequently, influences actual behavior. Carrington *et al.* (2014) identified other factors explaining the intention-action gap: prioritization of concerns, willingness to commit and sacrifice, formation of plans or even the impact of habits (Limayem *et al.*, 2007).

We could also explore the lack of concern of certain owner CEOs about security issues. A recent survey showed that small business owners are preoccupied with everyday business issues and often exhibit a lack of concern about information security problems, resulting in delayed or incorrectly implemented security measures (Bhattacharya, 2011). This result is consistent with another survey on SMEs and criminality that found interesting results on SME owners' risk perception and security behavior (Masurel, 2004). Even if there are different perceptions of the risk level according to industry, location and size, these dissimilarities do not lead to any significant differences in the levels of investment in security measures[6]: general investments in security are approximately one percent of a firm's sales. This lack of concern could also partially explain the low level of protection motivation. Future research should consider the question of how competences, available time, domains of interest, or other factors could influence the lack of concern of SME owners for implementing information security measures. Lauterbach and Vaninski (1999) and Hall and Nordqvist (2008) identified that these variables differentiated owners and non-owners regarding their SME efficiency (i.e., owner-managed firms were less efficient than firms managed by a professional non-owner manager). These criteria could be studied to see whether they also explain behavioral differences

[6] In this case, Masurel (2004) explicitly meant security and not information security.

between owner and non-owner CEOs in relation to information security.

In addition, an in-depth qualitative study could provide insights on additional relevant variables to address this very specific discrepancy between the two populations. In this context, a risk management method using the threat impact-probability approach could be adopted. We also may assume that other stakes (individual, cultural or institutional) may explain the behavioral differences we identified. We could examine mimetic mechanisms between owner CEOs and their peers (Barton *et al.*, 2016). Other variables, such as risk aversion or risk tolerance, could also provide insights on variations between SME CEOs' protection motivation. Specific ISS-related behaviors could be identified depending on the size of the firm (micro, small and medium-sized firms). Furthermore, the ownership structure and behavioral differences have been discussed in the literature on family businesses (Debicki *et al.*, 2009). These authors have indicated that ownership, especially in SMEs, may lead CEOs to partially overlap personal aspects with their business (Debicki *et al.*, 2009). From this more affective perspective, we could consider that vulnerability and social legitimacy may represent important aspects. While owner CEOs seem to be more impulsive-driven concerning perceived threats, non-owners seem to be more rational and base their reasoning more on efficacy. We propose investigating these affect and rationality dimensions in future research.

Our last avenue for future research would be to explore the role-sharing between actors (CEOs, CIOs, IT companies) in a more detailed manner and to include the notion of direct (doing) and indirect behavior (supporting the person who does) when the CEO does not act.

6.4. Managerial contributions

This study offers several implications for practice. As SMEs represent more than 99 percent of European companies, and given that CEOs' behavior influences employees' behavior and has a strong impact on SMEs' overall information security (Hu *et al.*, 2012), it is essential to encourage CEOs to act and communicate in favor of better protection of their information. Even if they lack IT skills, they should realize that taking security measures does not necessarily mean implementing formalized and expensive ISS measures. They sometimes just need to communicate with their employees about the importance of information security or set examples of good behavior (e.g., paying attention to eavesdropping or shredding confidential documents). Defining who is responsible for what information, establishing an information security committee, documenting information security processes, and preparing for an information security-related crisis are examples of actions that can be suggested to SME CEOs.

We found that SME owners' protection intention is highly explained by *social influence*. This implies that professional experts, such as certified public accountants (Barlette & Jaouen, 2014), institutions and all support structures that are part of the SME's ecosystem, may be aware of their role as advisors. They could help owners act, or at least they could raise their awareness about information protection. Such advice could be provided through training sessions or informal dialogue via social or professional networks. These training sessions could address the following issues: to increase the *perceived severity* of the risks, trainers could provide examples of security breaches and their actual impacts. To develop the *perceived vulnerability*, trainers could elaborate on the results of surveys to show that such incidents do not

"only happen to others" and demonstrate the increasing probability of attacks and their potential impacts on SMEs.

In addition, developing SME CEOs' knowledge in ISS would increase their perceptions of two distinct elements: (a) developing their skills in information technologies to foster their own feelings about their ability to implement information security measures (i.e., their *self-efficacy*) and (b) building on the efficacy of some basic protections (*response efficacy*) and the possibility of delegating (internally or externally) some important but maybe perhaps overly technical types of protections.

7. CONCLUSION

This research aimed to study the ISS behavior of SME CEOs, first through a general model and then with regard to the ownership of these firms. Using the protection motivation theory and based on data collected from 292 French SME CEOs, we tested constructs that explain their behavioral intention and actual behavior when engaging in protective information security measures.

The results showed that the antecedents of protective behavior were very different for owner and non-owner CEOs. The results for non-owners confirm and extend previous research on the protection motivation theory by focusing on a population that had not yet been specifically studied. Conversely, the results for SME owners were significantly different and highlighted the necessity of considering additional variables. For instance, the impact of social influence confirmed that factors other than the core PMT variables could influence their behavior. Consequently, we contribute to the knowledge on SME CEOs by showing that they must be distinctively addressed based on their ownership. It is of the utmost importance to dedicate more research to SME CEOs, as they constitute a specific and noteworthy population.

In a general way, based on the results of this research, we propose focusing future research, as well as managerial propositions, on actual behavior because understanding the final behavior – either best practices or their antecedents – is more relevant than behavioral intention for practitioners as well as academics.

ACKNOWLEDGEMENTS

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

REFERENCES

Ajzen, I. (1991), «The Theory of Planned Behavior», *Organizational Behavior & Decision Processes,* Vol. 50, n°2, p. 179-211.

Anderson, C.L., & Agarwal, R. (2010), «Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions», *MIS Quarterly,* Vol. 34, n°3, p. 613-643.

Anderson, E.E., & Choobineh, J. (2008), «Enterprise Information Security Strategies», *Computers & Security,* Vol. 27, n°1-2, p. 22-29.

Anderson, R., Dunkelberg, J., & Condon, C. (1990), «A Comparison of Entrepreneurs, Small Business Owners, Corporate Executives, and Public Sector Managers», *Journal of Business and Entrepreneurship,* Vol. 2, n°2, p. 41-50.

Anderson, R.C., & Reeb, D.M. (2003), «Founding-Family Ownership and Firm Performance: Evidence from the S&P 500», *Journal of Finance,* Vol. 58, n°3, p. 1301-1328.

Ashenden, D. (2008), «Information Security Management: A Human Challenge?» *Information Security Technical Report,* Vol. 13, n°4, p. 195-201.

Bandura, A. (1977), «Self-Efficacy: Toward a Unifying Theory of Behavioral Change», *Psychological Review,* Vol. 84, n°2, p. 191-215.

Bandura, A. (1994), "Self-Efficacy" in *Encyclopedia of Human Behavior*, V.S. Ramachandran (Ed), Academic Press, New York, NY, p. 71-81.

Barlette, Y. (2008), «Une Étude des Comportements Liés à la Sécurité des Systèmes D'information en PME», *Systèmes d'Information et Management,* Vol. 13, n°4, p. 7-30.

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°2, p. 115-149.

Barlette, Y., Gundolf, K., & Jaouen, A. (2015), «Toward a Better Understanding of SMB CEOs' Information Security Behavior: Insights from Threat or Coping Appraisal», *Journal of Intelligence Studies in Business,* Vol. 5, n°1, p. 5-17.

Barlette, Y., & Jaouen, A. (2014), "La Relation Entre le Dirigeant et Son Expert-Comptable en Matière de Gestion des Information" in *Le Grand Livre de L'économie PME 2015*, G. Lecointre (Ed), Gualino, Paris, p. 629-648.

Barton, K.A., Tejay, G., Lane, M., & Terrell, S. (2016), «Information System Security Commitment: A Study of External Influences on Senior Management», *Computers & Security,* Vol. 59, p. 9-25.

Bhattacharya, D. (2011), «Leadership Styles and Information Security in Small Businesses», *Information Management & Computer Security,* Vol. 19, n°5, p. 300-312.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., & Polak, P. (2015), «What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors», *MIS Quarterly,* Vol. 39, n°4, 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°2, p. 151-164.

Bruce, G., & Dempsey, R. (1997), *Security in Distributed Computing: Did You Lock the Door?* Hewlett Packard Company, Palo Alto, CA.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010), «Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness», *MIS Quarterly,* Vol. 34, n°3, p. 523-548.

Carland, J.W., Hoy, F., Boulton, W.R., & Jo Ann, C.C. (1984), «Differentiating Entrepreneurs from Small Business Owners: A Conceptualization», *Academy of Management Review,* Vol. 9, n°2, p. 354-359.

Carrington, M.J., Neville, B.A., & Whitwell, G.J. (2014), «Lost in Translation: Exploring the Ethical Consumer Intention-Behavior Gap», *Journal of Business Research,* Vol. 67, n°1, p. 2759-2767.

Chin, W.W. (1998), «The Partial Least Squares Approach to Structural Equation Modeling» in *Modern Methods for Business Research*, G.A. Marcoulides (Ed), Lawrence Erlbaum, Mahwah, NJ, p. 295-336.

Chu, A.M.Y., & Chau, P.Y.K. (2014), «Development and Validation of Instruments of Information Security Deviant Behavior», *Decision Support Systems,* Vol. 66, p. 93-101.

Ciborra, C. (2002), *The Labyrinths of Information: Challenging the Wisdom of Systems,* Oxford University Press, Oxford.

Courrent, J.-M., & Gundolf, K. (2009), «Proximity and Micro-Enterprise Manager's Ethics: A French Empirical Study of Responsible Business Attitudes», *Journal of Business Ethics,* Vol. 88, n°4, p. 749-762.

Cragg, P., Caldeira, M., & Ward, J. (2011), «Organizational Information Systems Competences in Small and Medium-Sized Enterprises», *Information & Management,* Vol. 48, n°8, p. 353-363.

Crossler, R.E., & Bélanger, F. (2014), «An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument», *Database for Advances in Information Systems,* Vol. 45, n°4, p. 51-71.

Crossler, R.E., Long, J.H., Loraas, T.M., & Trinkle, B.S. (2014), «Understanding Compliance with

Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap», *Journal of Information Systems,* Vol. 28, n°1, p. 209-226.

Dagorn, N. (2008), «Politiques en Matière de Sécurité des Systèmes D'information Inter-Organisationnels: Une Enquête dans Dix Grandes Entreprises», *Systèmes d'Information et Management,* Vol. 13, n°2, p. 97-125.

Dagorn, N., & Poussing, N. (2012), «Engagement et Pratiques des Organisations en Matière de Gouvernance de la Sécurité de l'Information», *Systèmes d'Information et Management,* Vol. 17, n°1, p. 113-143.

Dalton, D.R., Hitt, M.A., Certo, S.T., & Dalton, C.M. (2007), «Chapter 1: The Fundamental Agency Problem and Its Mitigation», *Academy of Management Annals,* Vol. 1, n°1, p. 1-64.

De Massis, A., Kotlar, J., Campopiano, G., & Cassia, L. (2015), «The Impact of Family Involvement on SMEs' Performance: Theory and Evidence», *Journal of Small Business Management,* Vol. 53, n°4, p. 924-948.

Debicki, B.J., Matherne, C.F., Kellermanns, F.W., & Chrisman, J.J. (2009), «Family Business Research in the New Millennium», *Family Business Review,* Vol. 22, n°2, p. 151-166.

Delone, W.H., & McLean, E.R. (2003), «The Delone and Mclean Model of Information Systems Success: A Ten-Year Update», *Journal of Management Information Systems,* Vol. 19, n°4, p. 9-30.

Dijkstra, T.K., & Henseler, J. (2015), «Consistent Partial Least Squares Path Modeling», *MIS Quarterly,* Vol. 39, n°2, p. 297-316.

Dinev, T., & Hu, Q. (2007), «The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies», *Journal of the Association for Information Systems,* Vol. 8, n°7, p. 386-408.

Dong, L. (2008), «Exploring the Impact of Top Management Support of Enterprise Systems Implementations Outcomes: Two Cases», *Business Process Management Journal,* Vol. 14, n°2, p. 204-218.

Dong, L., Neufeld, D., & Higgins, C. (2009), «Top Management Support of Enterprise Systems Implementations», *Journal of Information Technology,* Vol. 24, n°1, p. 55-80.

Drolet, A.L., & Morrison, D.G. (2001), «Do We Really Need Multiple-Item Measures in Service Research?» *Journal of Service Research,* Vol. 3, n°3, p. 196-204.

Dutta, A., & McCrohan, K. (2002), «Management's Role in Information Security in a Cyber Economy», *California Management Review,* Vol. 45, n°1, p. 67-87.

European Union. (2014), *Annual Report on European SMEs 2013-2014,* EU Publication Office.

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

Forcht, K.A., & Ayers, W.C. (2001), «Developing a Computer Security Policy for Organizational Use and Implementation», *Journal of Computer Information Systems,* Vol. 41, n°2, p. 52-57.

Fornell, C., & Bookstein, F.L. (1982), «Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory», *Journal of Marketing Research,* Vol. 19, n°4, p. 440-452.

Fornell, C., & Larcker, D.F. (1981), «Evaluating Structural Equation Models with Unobservable Variables and Measurement Error», *Journal of Marketing Research,* Vol. 18, n°1, p. 39-50.

Friend, M.A., & Pagliari, L.R. (2000), «Establishing a Safety Culture: Getting Started», *Professional Safety,* Vol. 45, n°5, p. 30-32.

Gamble, J.E., Lorenz, M.P., Turnipseed, D.L., & Weaver, K.M. (2013), «Determinants of Business Climate Perceptions in Small and Medium-Sized Enterprises: Does Managerial Ownership Matter?» *Small Business Institute Journal,* Vol. 9, n°1, p. 18-36.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000), «Structural Equation Modeling and Regression: Guidelines for Research Practice», *Communications of the AIS,* Vol. 4, n°1, p. 7.

Gupta, A., & Hammond, R. (2005), «Information Systems Security Issues and Decisions for Small Businesses: An Empirical Examination», *Information Management and Computer Security,* Vol. 13, n°4, 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.

Gustke, C. (2016), «No Business Too Small to Be Hacked», *New York Times*, http://www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0, accessed May 9, 2017.

Hair, J.F., Hult, G.T.M., Ringle, C., & Sarstedt, M. (2017), *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», *Journal of Marketing Theory and Practice,* Vol. 19, n°2, p. 139-152.

Hall, A., & Nordqvist, M. (2008), «Professional Management in Family Businesses: Toward an Extended Understanding», *Family Business Review,* Vol. 21, n°1, p. 51-69.

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°1, 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°1, p. 2-20.

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°2, p. 154-165.

Ho, R. (2000), «Predicting Intention for Protective Health Behaviour: A Test of the Protection Versus the Ordered Protection Motivation Model», *Australian Journal of Psychology,* Vol. 52, n°2, p. 110-118.

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°4, 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°1, p. 83-95.

James, H.S. (1999), «Owner as Manager, Extended Horizons and the Family Firm», *International Journal of the Economics of Business,* Vol. 6, n°1, p. 41-55.

Jaouen, A., & Lasch, F. (2015), «A New Typology of Micro-Firm Owner-Managers», *International Small Business Journal,* Vol. 33, n°4, p. 397-421.

Jarvenpaa, S.L., & Ives, B. (1991), «Executive Involvement and Participation in the Management of Information Technology», *MIS Quarterly,* Vol. 15, n°2, p. 205-227.

Jensen, M.C., & Meckling, W.H. (1976), «Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure», *Journal of Financial Economics,* Vol. 3, n°4, p. 305-360.

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°1, p. 113-134.

Jones, O. (2003), «The Persistence of Autocratic Management in Small Firms: TCS and Organisational Change», *International Journal of Entrepreneurial Behavior & Research,* Vol. 9, n°6, p. 245-267.

Jöreskog, K.G. (1971), «Statistical Analysis of Sets of Congeneric Tests», *Psychometrika,* Vol. 36, n°2, p. 109-133.

Julien, P.-A. (1990), «Vers une Typologie Multicritère des PME», *Revue Internationale PME,* Vol. 3, n°3-4, p. 411-425.

Kankanhalli, A., Teo, H.-H., Tan, B.C., & Wei, K.-K. (2003), «An Integrative Study of Information Systems Security Effectiveness», *International*

Journal of Information Management, Vol. 23, n°2, p. 139-154.

Kayworth, T., & Whitten, D. (2010), «Effective Information Security Requires a Balance of Social and Technology Factors», *MIS Quarterly Executive,* Vol. 9, n°3, p. 163-175.

Keeper. (2016), *2016 State of Cybersecurity in Small & Medium-Sized Businesses*, June.

Kim, S.H., Jang, S.Y., & Yang, K.H. (2017), «Analysis of the Determinants of Software-as-a-Service Adoption in Small Businesses: Risks, Benefits, and Organizational and Environmental Factors», *Journal of Small Business Management,* Vol. 55, n°2, p. 303-325.

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°1, p. 24-36.

Komatsu, A., Takagi, D., & Takemura, T. (2013), «Human Aspects of Information Security: An Empirical Study of Intentional Versus Actual Behavior», *Information Management & Computer Security,* Vol. 21, n°1, p. 5-15.

Kotulic, A.G., & Clark, J.G. (2004), «Why There Aren't More Information Security Research Studies», *Information & Management,* Vol. 41, n°5, p. 597-607.

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.

Lauterbach, B., & Vaninsky, A. (1999), «Ownership Structure and Firm Performance: Evidence from Israel», *Journal of Management and Governance,* Vol. 3, n°2, p. 189-201.

Lee, Y. (2011), «Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective», *Decision Support Systems,* Vol. 50, n°2, 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°2, p. 177-187.

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°1, 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°7, p. 394-413.

Limayem, M., Hirt, S.G., & Cheung, C.M. (2007), «How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance», *MIS Quarterly,* Vol. 31, n°4, p. 705-737.

Lorenz, M.P., Gamble, J.E., Turnipseed, D.L., & Weaver, K.M. (2015), «Do Owners and Managers Really Differ? An Examination of Satisfaction with Overall Firm Performance in Small- and Medium-Sized Enterprises» *International Journal of Entrepreneurship and Innovation*, Vol. 16, n°3, p. 1-11.

Lucas, H.C. (1981), *Implementation: The Key to Successful Information Systems,* Columbia University Press, New York, NY.

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°5, p. 469-479.

Markus, M.L. (1983), «Power, Politics, and MIS Implementation», *Communications of the ACM,* Vol. 26, n°6, p. 430-444.

Masurel, E. (2004), «SMEs and Crime: Evidence from the Netherlands», *International Small Business Journal,* Vol. 22, n°2, p. 197-205.

Michaelas, N., Chittenden, F., & Poutziouris, P. (1999), «Financial Policy and Capital Structure Choice in UK SMES: Empirical Evidence from Company Panel Data», *Small Business Economics,* Vol. 12, n°2, p. 113-130.

Mijnhardt, F., Baars, T., & Spruit, M. (2016), «Organizational Characteristics Influencing SME Information Security Maturity», *Journal of Computer Information Systems,* Vol. 56, n°2, p. 106-115.

Miller, D., Breton-Miller, L., & Scholnick, B. (2008), «Stewardship vs. Stagnation: An Empirical Comparison of Small Family and Non-Family Businesses», *Journal of Management Studies,* Vol. 45, n°1, p. 51-78.

Mills, C., & Pawson, K. (2012), «Integrating Motivation, Risk-Taking and Self-Identity: A Typology of ICT Enterprise Development Narratives», *International Small Business Journal,* Vol. 30, n°5, p. 584-606.

Neuwirth, K., Dunwoody, S., & Griffin, R.J. (2000), «Protection Motivation and Risk Communication», *Risk Analysis,* Vol. 20, n°5, p. 721-734.

Ng, B.-Y., Kankanhalli, A., & Xu, Y.C. (2009), «Studying Users' Computer Security Behavior: A Health Belief Perspective», *Decision Support Systems,* Vol. 46, n°4, p. 815-825.

Njenga, K., & Jordaan, P. (2016), «We Want to Do It Our Way: The Neutralisation Approach to Managing Information Systems Security by Small Businesses», *African Journal of Information Systems,* Vol. 8, n°1, p. 42-63.

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°2, 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 et Management,* Vol. 8, n°4, p. 87-118.

Perks, S. (2010), «Problem-Solving Techniques of Growing Very Small Businesses», *Journal of Enterprising Communities: People and Places in the Global Economy,* Vol. 4, n°3, p. 220-233.

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°5, p. 879-903.

Podsakoff, P.M., & Organ, D.W. (1986), «Self-Reports in Organizational Research: Problems and Prospects», *Journal of Management,* Vol. 12, n°4, p. 531-544.

Poutziouris, P. (2003), «The Strategic Orientation of Owner-Managers of Small Ventures: Evidence from the UK Small Business Economy», *International Journal of Entrepreneurial Behavior & Research,* Vol. 9, n°5, p. 185-214.

Pritchard, S. (2010), «Navigating the Black Hole of Small Business Security», *Infosecurity,* Vol. 7, n°5, p. 18-21.

Prnewswire. (2015), «Small and Midsized Businesses Learn to Protect Their Digital Assets During National Cyber Security Awareness Month», http://www.prnewswire.com/news-releases/small-and-midsized-businesses-learn-to-protect-their-digital-assets-during-national-cyber-security-awareness-month-300154074.html, accessed May 9, 2017.

Puhakainen, P., & Siponen, M. (2010), «Improving Employees' Compliance through Information Systems Security Training: An Action Research Study», *MIS Quarterly,* Vol. 34, n°4, p. 757-778.

PWC. (2014), *The Global State of Information Security Survey 2015: Managing Cyber-Risks in an Interconnected World.*

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°2, p. 100-108.

Raymond, L., & Magnenat-Thalmann, N. (1982), «Information Systems in Small Business: Are They Used in Managerial Decisions?», *American Journal of Small Business,* Vol. 6, n°4, p. 20-26.

Rees, J. (2010), «Information Security for Small and Medium-Sized Business», *Computer Fraud & Security,* Vol. 2010, n°9, p. 18-19.

Reid, R.C., & Gilbert, A.H. (2009), «Cognitive Support for Senior Manager's Decision Making in Information Systems Security», *Proceedings of the Academy of Information and Management Sciences,* Vol. 13, n°1, p. 58-62.

Robinson, S., & Volonino, L. (2004), *Principles and Practices of Information Security,* Pearson Prentice Hall, New Jersey.

Rockart, J.F., & Crescenzi, A.D. (1984), «Engaging Top Management in Information Technology», *Sloan Management Review,* Vol. 25, n°4, p. 3-16.

Rogers, R.W. (1975), «A Protection Motivation Theory of Fear Appeals and Attitude Change», *The Journal of Psychology,* Vol. 91, n°1, p. 93-114.

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

Ross, J.W., & Weill, P. (2002), «Six It Decisions Your It People Shouldn't Make», *Harvard Business Review,* Vol. 80, n°11, p. 84-91.

Ross, S.A. (1973), «The Economic Theory of Agency: The Principal's Problem», *The American Economic Review,* Vol. 63, n°2, p. 134-139.

Ryan, J.J.C.H. (2004), «Information Security Tools and Practices: What Works?», *IEEE Transactions on Computers,* Vol. 53, n°8, p. 1060-1063.

Schoonjans, B., Van Cauwenberge, P., & Vander Bauwhede, H. (2013), «Formal Business Networking and SME Growth», *Small Business Economics,* Vol. 41, n°1, p. 169-181.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014), «Employees' Adherence to Information Security Policies: An Exploratory Field Study», *Information & Management,* Vol. 51, n°2, p. 217-224.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015), «The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance», *Information and Computer Security,* Vol. 23, n°2, p. 200-217.

Stewart, W.H., Watson, W.E., Carland, J.C., & Carland, J.W. (1999), «A Proclivity for Entrepreneurship: A Comparison of Entrepreneurs, Small Business Owners, and Corporate Managers», *Journal of Business Venturing,* Vol. 14, n°2, p. 189-214.

Straub, D., Limayem, M., & Karahanna-Evaristo, E. (1995), «Measuring System Usage: Implications for is Theory Testing», *Management Science,* Vol. 41, n°8, p. 1328-1342.

Taylor, R.G., & Brice, J. (2012), «Fact or Fiction? A Study of Managerial Perceptions Applied to an Analysis of Organizational Security Risk», *Journal of Organizational Culture, Communications and Conflict,* Vol. 16, n°1, p. 1-23.

Torrès, O., & Julien, P.-A. (2005), «Specificity and Denaturing of Small Business», *International Small Business Journal,* Vol. 23, n°4, p. 355-377.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012), «Analyzing Trajectories of Information Security Awareness», *Information Technology & People,* Vol. 25, n°3, p. 327-352.

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°4, 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°3–4, p. 190-198.

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

Vermeulen, C., & Solms, R.V. (2002), «The Information Security Management Toolbox – Taking the Pain out of Security Management», *Information Management & Computer Security,* Vol. 10, n°3, p. 119-125.

Wagener, S., Gorgievski, M., & Rijsdijk, S. (2010), «Businessman or Host? Individual Differences between Entrepreneurs and Small Business Owners in the Hospitality Industry», *The Service Industries Journal,* Vol. 30, n°9, p. 1513-1527.

Williams, P. (2007), «Executive and Board Roles in Information Security», *Network Security,* Vol. 2007, n°8, p. 11-14.

Wolcott, P., Kamal, M., & Qureshi, S. (2008), «Meeting the Challenges of ICT Adoption by Micro-Enterprises», *Journal of Enterprise Information Management,* Vol. 21, n°6, p. 616-632.

Woon, I.M.Y., Tan, G.W., & Low, R.T. (2005), "A Protection Motivation Theory Approach to Home Wireless Security" in *Twenty-Sixth International Conference on Information Systems*, Las Vegas.

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°6, p. 2799-2816.

Yoon, C., & Kim, H. (2013), «Understanding Computer Security Behavioral Intention in the Workplace: An Empirical Study of Korean Firms», *Information Technology & People,* Vol. 26, n°4, p. 401-419.

Zwikael, O. (2008), «Top Management Involvement in Project Management: Exclusive Support Practices for Different Project Scenarios», *International Journal of Managing Projects in Business,* Vol. 1, n°3, p. 387-403.

APPENDIXES

APPENDIX A: NON-CORE PMT & NON-IS STUDIES

In our paper, we built Table 1 based on Boss *et al.*'s Table A1 (2015, p. A2) using the following criteria:

The journal had to pertain to the IS field.

The journal had to be ranked in CNRS or FNEGE rankings, assuming that the most important IS international journals are included in those rankings.

The articles had to address "core PMT," as defined by Boss *et al.* (2015).

These interesting studies, although not in line with our criteria, were moved into this appendix:

- Workman *et al.*, 2008 (Computers in Human Behavior, not in the IS field and old);
- Gurung *et al.*, 2009 (IMCS, not in the IS field and old);
- Herath & Rao, 2009 (EJIS, but no use of core PMT);
- Anderson & Agarwal, 2010 (MISQ, but no use of core PMT);
- Yoon & Kim, 2013 (CSV, not in the IS field, no use of core PMT);
- Crossler *et al.*, 2014 (Journal of Information Systems, not ranked);
- Johnston *et al.*, 2015 (MISQ, but no use of core PMT);
- Tu *et al.*, 2015 (I&M, but no use of core PMT);
- Hanus & Wu, 2016 (Information Systems Management, not ranked).

Papers	Year	Target & Company Size	Behavioral Intention	Actual Behavior
Workman *et al.*	2008	Employees Large IT firm	N/A	Take measures to protect information (subjective) + logs (objective)
Gurung *et al.*	2009	**Students**	N/A	Use of anti-spyware
Herath & Rao	2009	Employees All Sizes	Compliance with Orga ISSP	N/A
Anderson & Agarwal	2010	Public Users + **Students**	Protect the Internet Protect one's own PC	N/A
Yoon & Kim	2013	Employees All Sizes	Take measures to protect information	N/A
Crossler *et al.*	2014	**Students** & Professionals	BYOD policy compliance	
Johnston *et al.*	2015	Employees City Govt	Changing Passwords	N/A
Tu *et al.*	2015	Public Users	Take measures to protect mobile devices	N/A
Hanus & Wu	2016	**Students**	N/A	Use & update antivirus + firewall

None of these studies examines the impact of PMT constructs on behavioral intention and at the same time on actual behavior.

APPENDIX B: ANALYSIS OF VARIABLE SIGNIFICANCE AND INFLUENCE

			"Core" Protection Motivation Theory					
	Authors	Date	Perceived Severity	Perceived Vulnerability	Response Efficacy	Self Efficacy	Cost	Social Influence
BI->AB	Lee & Larsen (Non IT)	2009	+	NS	+	+	+	NS
	Lee & Larsen (Global)		+	+				+
BI	Jonhston & Warkentin	2010	-	NS	+	+	N/A	+
BI->AB	Liang & Xue	2010	+	+	+	+	+	N/A
BI->AB	Lee	2011	+	+	+	+	+	NS
BI	Ifinedo	2012	-	+	+	+	NS	+
BI	Vance et al.	2012	+	NS	-	+	+	N/A
AB	Crossler et Belanger	2014	+	-	+	+	NS	N/A
BI->AB	Siponen et al.	2014	+	+	NS	+	NS	+
BI->AB	Boss et al. (backups)	2015	+	NS	NS	NS	+	N/A
	Boss et al. (antivirus)		NS		+			
BI->AB	Our study (All)	2016	NS	NS	+	+	-	+
	Our study (Owners)			+	NS	NS		NS
	Our study (non-owners			NS	+	+		+

Studies using PMT with important changes in the PMT model or in the variables

			SEV	VULN	REFF	SEFF	COST	SINFL	Other Vars
AB	Workman et al. (IT)	2008	+	+	+	+	+	N/A	Locus control
AB	Gurung et al.	2009	+	NS	+	+	NS	N/A	
BI	Herath & Rao	2009	N/A	NS	N/A	+	N/A	+	Many
BI	Anderson & Agarwal	2010	+	N/A	+	+	N/A	NS (Web); + (Own PC)	Many
BI	Yoon & Kim	2013	+	NS	+	+	N/A	NS	Many
BI = AB	Crossler et al.	2014	+	NS	+	+	NS	N/A	
BI	Tu et al.	2015	+		+	+	N/A	+	Other
BI	Johnston et al.	2015	+	NS	+	+	N/A	N/A	Many (GDT)
AB	Hanus & Wu	2016	NS	NS	+	+	NS	N/A	Awareness

GDT: General Deterrence Theory
IT: Mainly IT people
NS: Non Significant
N/A: Not applicable
- : Effect is reverse than expected

APPENDIX C: MOST USED CONTROL – DEMOGRAPHIC VARIABLES

Studies using core PMT variables

Authors	Date	Gender	Age	Seniority in position	Position (Owner)	Size	Educ	Industry	IT or ISS Budget	Internet Exp (Y)	Mobile Exp (Y)	Comput Exp (Y)	Number of users	Specific Vars
Lee & Larsen	2009				X	X		X	X					
Jonhston & Warkentin	2010	X	X	X			X							
Liang & Xue	2010	X	X							X				
Lee	2011	X	X	X	X									Class size, Load
Ifinedo	2012	X	X		X	X	X							Industry revenue
Vance et al.	2012	X												Scenario
Crossler et Belanger	2014		X	X								X		
Siponen et al.	2014	X		X										
Boss et al.	2015	X	X									X		
Number of occurrences		7	6	4	3	2	2	1	1	1	0	2	0	

Studies using PMT with important changes in the PMT model or in the variables

Workman et al.	2008	No mention of control variables												
Gurung et al.	2009	X								X				
Herath & Rao	2009	X	X	X	X	X	X	X	X				X	
Anderson & Agarwal	2010	X	X		X					X				Freq PB
Yoon & Kim	2013	X	X	X	X	X		X						
Crossler et al.	2014	X	X	X	X						X			
Tu et al.	2015	X	X											Mobile Type
Johnston et al.	2015	X	X	X		X								
Number of occurrences		8	6	3	4	2	2	2	1	2	1	0	1	

APPENDIX D: VARIABLES AND ITEMS

	Variable	Reference	Item	Code
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.	REFF1
			If I take in charge information security in my company, it will limit the impact of an information security problem.	REFF2
		Vance et al., 2012	Even if I complied with information security policies, information security problems could not be avoided (Reverse-coded item).	REFF3 (dropped)
	Self-efficacy	Vance et al., 2012 Ifinedo, 2012	I can implement information security measures by myself.	SEFF1
			Implementing information security measures is easy for me.	SEFF2
		Lent et al. 2006 Ifinedo, 2012	I have the capability to solve problems during the implementation of security measures.	SEFF3
	Response cost	Vance et al., 2012	Complying with information security policies requires considerable investment of effort other than time.	COST1
			There are too many overheads associated with complying with information security policies.	COST2
			Complying with information security policies inconveniences my work.	COST3
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.	SEV1
			If my computerized data were temporarily not available, serious information security problems would result.	SEV2
			An information security breach would have a serious negative impact for my company.	SEV3
	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.	VULN1
			My personal data could be subject to a threat if I did not apply information security policies.	VULN2
			My company could be subject to a threat if I did not apply information security policies.	VULN3
Social Influence		Ho, 2000; Lee & Larsen, 2009; Anderson & Agarwal, 2010	My competitors have adopted or are in the process of adopting information security measures.	SINFL1
			My partner companies believe I should adopt information security measures.	SINFL2
			My customers believe I should adopt information security measures to protect their own customer data.	SINFL3
Behavioral intention		Workman et al., 2008 Yoon & Kim, 2013	I intend to implement information security measures in the next months.	BI1
			I plan to implement security measures in the next months.	BI2
Actual Behavior		Workman et al., 2008 Yoon & Kim, 2013	I have implemented information security measures in my company.	AB_Gen
Ownership		Position (Lee, 2011)	Non-owner = 0; Owner = 1	OWNER
Control Variables	Age	Liang & Xue, 2010; Boss et al., 2015	Age	AGE
	Gender		Male =0; Female =1	GENDER
	Seniority in position	Crossler & Belanger, 2014; Siponen et al., 2014	Number of years	SENIOR
	Firm Size	Ifinedo, 2012 Lee & Larsen, 2009	Number of employees (0 - 250)	SIZE

APPENDIX E: COMMON METHOD BIAS ASSESSMENT

Summary of Liang *et al.*'s (2007, Appendix E, p.85-87) approach:

We converted each indicator to a single-indicator latent construct. Consequently, all our variables became second-order constructs. The latent method factor was also created as a second-order construct that was linked to all of the single-indicator constructs. For each single-indicator construct, we compared the coefficients of its two incoming paths, one from its substantive (original) construct and one from the (new) method factor. If the method factor loadings are insignificant and the indicator's substantive variances are greater than their method variances, we can assume that common method bias is not a serious concern.

Construct	Indicator	Substantive Factor Loading (R1)	$R1^2$	Method Factor Loading (R2)	$R2^2$
SEV	SEV1	0,816**	0,666	0,023	0,001
	SEV2	0,814**	0,663	0,079*	0,006
	SEV3	0,902**	0,814	-0,11**	0,012
VULN	VULN1	0,888**	0,789	0,003	0,000
	VULN2	0,893**	0,797	0,001	0,000
	VULN3	0,858**	0,736	-0,004	0,000
REFF	REFF1	0,914**	0,835	0,032	0,001
	REFF2	0,954**	0,910	-0,033	0,001
SEFF	SEFF1	0,88**	0,774	-0,038	0,001
	SEFF2	0,925**	0,856	0,013	0,000
	SEFF3	0,881**	0,776	0,023	0,001
COST	COST1	0,779**	0,607	0,111**	0,012
	COST2	0,858**	0,736	-0,122**	0,015
	COST3	0,841**	0,707	0,008	0,000
SINFL	INFL1	0,737**	0,543	0,081	0,007
	INFL2	0,942**	0,887	-0,051	0,003
	INFL3	0,898**	0,806	-0,021	0,000
BI	BI1	0,943**	0,889	0,011	0,000
	BI2	0,956**	0,914	-0,011	0,000
AB	AB_Gen	1,000	1,000	0,000	0,000
Average		0,878	0,774	0,000	0,003

*p < .05; **p < .01

APPENDIX F: PERMUTATION AND MULTI-GROUP TESTS

Results of permutation tests (owners vs. non-owners)

Latent Variables	Difference	P	Significance
SEV -> BI	0,181	0,149	No
VULN -> BI	0,261	0,020	Yes
REFF -> BI	0,204	0,079	No
SEFF -> BI	0,271	0,030	Yes
COST -> BI	0,035	0,772	No
SINFL -> BI	0,165	0,178	No
BI -> AB	0,366	0,010	Yes

Results of multi-group tests

Variable	Values	Group Size	%
OWNER	0	109	37.33
	1	183	62.67

Path coefficient	Groups	Difference	Observed value	Critical Value	DoF	p-value	Significant
VULN -> BI	1 vs 0	0.261	1.991	1.968	290	0.047	Yes
SEV -> BI	1 vs 0	0.181	1.384	1.968	290	0.167	No
VULN -> BI	1 vs 0	0.261	1.991	1.968	290	0.047	Yes
REFF -> BI	1 vs 0	0.204	1.397	1.968	290	0.163	No
SEFF -> BI	1 vs 0	0.271	1.615	1.968	290	0.107	No
COST -> BI	1 vs 0	0.035	0.262	1.968	290	0.793	No
SINFL -> BI	1 vs 0	0.165	1.354	1.968	290	0.177	No
BI -> AB	1 vs 0	0.366	3.177	1.968	290	0.001	Yes