Available for free online at https://ojs.hh.se/

Journal of Intelligence Studies in Business Vol 5, No 1 (2015) 5-17

Toward a better understanding of SMB CEOs' Information Security Behavior: Insights from Threat or Coping appraisal

Yves Barlette[1], Katherine Gundolf[1], Annabelle Jaouen[1]

[1] Montpellier Business School, France

Email: y.barlette@montpellier-bs.com
k.gundolf@montpellier-bs.com
a.jaouen@montpellierbs.com

Received March 15, accepted May 16 2015

ABSTRACT: This study presents an empirical investigation of factors affecting SMB CEOs decision to improve or not their company's information security (ISS). We developed a research model by adopting the protection motivation theory (PMT) to investigate the effect of threat and coping appraisal on protective actions. We conducted a questionnaire-based survey with SMB CEOs. Prior studies using PMT have never been focused on SMB CEOs behavior, and we postulate that in SMBs where there is no CIO or even IT people, CEO's actions are of utmost importance for achieving a satisfying ISS.

KEYWORDS: Protection Motivation Theory, Coping, CEO, SMB, Behavior, Information Security.

1. Introduction

Many threats to information security (ISS) come from employees' behavior which are not compliant with information security policies (Chu & Chau, 2014; Siponen et al., 2014), ISS organizational rules or even guidelines or requirements (Ifinedo, 2012; Workman et al., 2008). However, numerous surveys and studies have confirmed that managerial support is essential in obtaining adherence of employees to ISS (Avolio, 2000; Johnston & Hale, 2009). In addition, employees' involvement and propensity to act are directly dependent on managers' concrete actions (Dong et al., 2009; Forcht & Ayers, 2000).

To date, little attention has been given to top management's role. Withal, many scholars advocated that ISS should be addressed at the top management level (Markus, 1983; Longeon & Archimbaud, 1999; Friend & Pagliari, 2000; Knapp et al., 2006).

The MIS literature repeatedly shows that managers must not only be aware but also be personally involved. Managers' involvement is essential in the implementation, maintenance and success of ISS-related actions (Johnston & Hale, 2009). Rockart & Crescenzi (1984) declared that managers must recognize that information is a strategic resource and that *"senior executives are increasingly feeling the need to become informed, energized, and engaged in information systems*" (p.3). Top managers must be considered as the starting point for satisfactory ISS (Robinson & Volonino, 2004). According to Longeon & Archimbaud (1999): *"determining and supervising the security policy are top management concerns. Nothing valuable can be done without the manager, provided that he knows all the challenges involved."* (p. 19). However, some managers are poorly involved or are poorly acting in their company's ISS, leading to potentially disastrous consequences.

Few studies aimed at understanding CEOs' participation and actions in ISS (Dong, 2008; Zwikael, 2008; Barlette, 2012). Moreover, studies dedicated to factors influencing action, their incidence on ISS, and major actions that are incumbent to managers usually focus on medium or large business executives (Lee and Larsen, 2009; Vance et al., 2012).

This study investigates ISS in French SMBs. In 2013, SMBs (less than 250 employees) accounted for 99.8% of all enterprises active in the EU28 non-financial business sector, representing 66.8% of total employment, including a large part of small (less than 50 employees) and micro-enterprises (less than 10) (European Commission, 2014). ISS surveys have revealed that SMBs are far behind larger companies in implementing protection because they lack technical (Labodi & Michelberger, 2010) and financial resources (Lee & Larsen, 2009). SMBs have to face important issues: (1) it is more difficult for SMBs to recruit and keep ICT or ISS specialists (Monnoyer, 2003; Pritchard, 2010), (2) ongoing risk assessment is often lacking (Gupta & Hammond, 2005), and (3) many SMB managers are not sufficiently aware of ISS issues (Mitchell et al., 1999) and consider information security to be a 'large business' concern (Rees, 2010). The unfortunate truth is that SMBs are as much – and in some cases more – at risk from security breaches that could threaten their organization (Rees, 2010). Therefore, SMBs and their managers constitute a specific case for ISS research. In this study we test protection motivation theory (PMT) on SMB CEOs and observe what factors explain their intention to engage in protective actions for their firm.

This paper is structured as follows: in section two, the literature review will lead to our model and hypotheses development. Third section introduces our methodology. We present our results in the fourth section and discuss them in section five. In the last section, we sum up our main results and introduce our next study.

2. Research background

In this section, we will introduce successively protection motivation theory, then our model and hypotheses.

2.1. Protection motivation theory (PMT)

PMT (Rogers, 1983) is one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson & Agarwal, 2010). PMT can be divided into two major components: threat appraisal and coping appraisal factors.

2.1.1. Threat appraisal

The perception of threat is defined as the anticipation of a psychological, sociological or physical violation or harm to oneself or others (Lazarus, 1991; Workman et al., 2008). People perceiving this threat will adjust their behavior according to the amount of risk they are willing to accept. This adjustment is based on the perceived severity of cost and damage associated with the threat and their perceived vulnerability related to the threat.

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

Perceived severity corresponds to the perception of the severity of the consequences of an ISS problem, because ISS measures were insufficient or ineffective (Ifinedo, 2012; Liang & Xue, 2010). It includes for example the perceived level of company's loss of activity, loss of data, financial losses and the eventual 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, e.g. people will be less cautious if the perceived severity diminishes (Bulgurcu et al., 2010; Herath & Rao, 2009).

2.1.2. Coping appraisal

Coping behavior will depend on the control perceived by people on this behavior, their perceived capabilities, and the effort they will expend to accomplish that behavior (Bandura, 1977). Three components will influence this coping appraisal: response efficacy, self-efficacy and response cost.

Response efficacy corresponds to the beliefs about the perceived benefits of the behavior exerted by the individual (Rogers, 1983). If people perceive the available coping mechanisms as adequate, for example because available security measures are improving (Kankanhalli et al., 2003), they are less likely to omit an ISS-related behavior. On the contrary, if people have a negative perception of the efficacy of the necessary behavior, because no matter what they do security breaches will go on increasing, they will be more likely to omit this behavior (Workman et al., 2008).

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).

Prior research has demonstrated people are more motivated to cope with or perform IT security behaviors as the level of their self-efficacy increases (Workman et al., 2008).

Response cost resembles to the physical and cognitive efforts necessary for the adaptive response (Lian & Xue, 2010). It can correspond to money or time to invest in the behavior or the security measure, the inconvenience or the difficulty of the behavior itself. This perceived effort is put into balance with the perceived value of the ISS-related behavior (Workman et al., 2008).

2.2. The research model and hypotheses

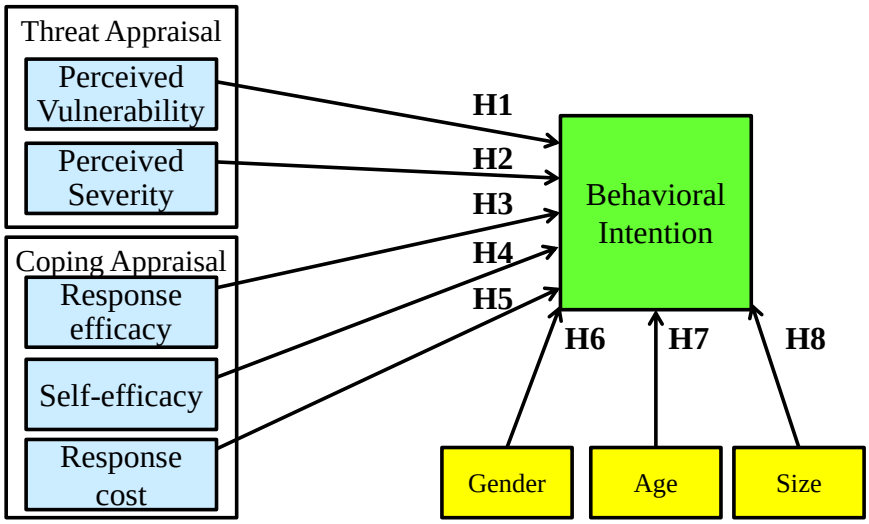

Figure 1. The theoretical model

Threat appraisal: An increase in perceived severity and vulnerability leads to greater intention to behave in a healthier manner. Therefore we postulated (see Fig. 1):

- *H1: Perceived severity of potential information security threats influences positively and significantly SMB CEOs' intention to perform information security-related actions.*
- *H2: Perceived vulnerability from potential information security threats influences positively and significantly SMB CEOs' intention to perform information security-related actions.*

Coping appraisal: according to PMT, it consists of self-efficacy, response-efficacy and response cost.

Response efficacy, in the context of our research, refers to the CEOs' belief in whether performing information security-related actions can enhance their company's security and reduce security flaws.

We postulated:

- *H3: Response efficacy to potential information security threats influences positively and significantly SMB CEOs' intention to perform information security-related actions.*

Self-efficacy referred here to CEOs' belief in their ability to perform information security-related actions. We believe that self-efficacy to potential information security threats has a positive and significant impact on CEOs' intention to perform information security-related actions.

We therefore postulated:

- *H4: Self-efficacy to potential information security threats influences positively and significantly SMB CEOs' intention to perform information security-related actions.*

Response cost represents any costs (e.g. time, monetary, difficulty, complexity, effort) associated with taking the adaptive coping response. Hence, we postulated:

- *H5: Response cost influences negatively SMB CEOs' intention to perform information security-related actions.*

Gender has been found to be important in IT contexts (Venkatesh et al., 2003). Therefore we postulated:

- *H6: Male SMB CEOs have a greater intention to perform information security-related actions than female CEOs.*

Age showed significant differences in the involvement of managers and their perception of troubles affecting their company's IS (Stevens et al., 1978, Venkatesh et al., 2003). Thus, we posited:

- *H7: Age negatively affects SMB CEOs' intention to perform information security-related actions.*

Lee and Larsen (2009) did not identify that the size had any significant influence on the behavioral intention. Anyway, we posit that the smaller the size of the company, the more important the role of the CEO in the management of information security. Thus, we postulate that a larger firm's size is negatively related with CEO's behavioral intention to take or implement I.S. security measures.

- *H8: Company's size influences negatively SMB CEOs' intention to perform information security-related actions.*

3. Methodology

3.1. Research design

The research model was tested using a field survey. We administrated the questionnaire to SMB CEOs. Each participant received an email explaining the purpose of our study, including a link to our web-based questionnaire. A total of 258 responses were returned between December 2014 and January 2015. After removing incomplete and invalid responses, we obtained 177 usable responses. Response rates for information security-related surveys are usually low (Kotulic & Clark, 2004). In addition, SMB 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 Appendix A) were taken from previously validated research. The response efficacy and perceived severity scales (*Eff. R, Sev.*) had measures adapted from Vance et al. (2012). The self-efficacy scale (*Eff. S*) had measures borrowed from Lent et al. (2006) and Vance et al. (2012). The response cost and perceived vulnerability scales (*Cost, Vuln*) had measures borrowed from Vance et al. (2012). The behavioral intention scale (*Int.*) used measures adapted form Workman et al. (2008) and Yoon and Kim (2013).

All items, except nominal variables, were measured using 7-point Likert scales anchored at 1="Strongly disagree" and 7="Strongly agree". The questions included in our instrument were first pre-tested through face-to-face interviews with SMB CEOs (N=14). Based on CEOs' feedback, the readability of the questions was improved.

The questionnaire itself was created using Qualtrics tool. In the beginning of the questionnaire, an introductory text defined information security and specifying 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.

3.2. Measures

Our purpose was to determine the influence of antecedents on behavioral intention. All the items of the questionnaire are described in Appendix A.

Dependent variable

The dependent variable Behavioral Intention *(Int.)* was calculated through a factorized construct (Cronbach's alpha = 0.904) composed of two items, *Int1* and *Int2*.

Independent variables

The independent variables were divided into two groups. To measure threat appraisal, we observed perceived vulnerability (*Vuln.*) and perceived severity (*Sev.*). To measure coping appraisal, we used three variables: response efficacy (*Eff. R.)*, self-efficacy (*Eff. S.*), response cost (*Cost.*). All items exhibited a reliability score over 0.7, which is considered as satisfying.

	Variable	Factorized construct	Cronbach's alpha	Items (see Appendix A)
Threat appraisal	Perceived vulnerability	*Vuln*	0.857	*Vuln1, Vuln2, Vuln3*
	Perceived severity	*Sev*	0.770	*Sev2, Sev3*
Coping appraisal	Response efficacy	*Eff. R*	0.795	*Eff. R1, Eff. R2*
	Self-efficacy	*Eff. S*	0.899	*Eff. S1, Eff. S2, Eff. S3*
	Response cost	*Cost*	0.712	*Cost1, Cost2, Cost3*

Table 1: Constructs and reliability of measurement items

Control variables

As control variables, we included *Gender*, *Size* and *Age*. We included gender in the form of a dummy variable (male = 0; female = 1). Size was measured through a scale according to the European classification of firms: less than ten employees (micro-enterprises = 1), ten up to 49 employees (small enterprises = 2) and 50 up to 250 employees

(medium enterprises = 3). Age represents the respondent's age.

3.3. Data analysis

To test the hypotheses, a multiple regression analysis was performed using the statistical analysis software SPSS (version 21). In doing so, we performed regressions of the control variables size, age and gender as well as the independent variables, on CEO's behavioral intention, our model's dependent variable. The common method bias was controlled by a Harman's single factor test (Podsakoff et al., 2003). The most covariance explained by one factor in our data is 17.6 percent; hence CMV bias was not a problem for our data.

4. Results

As showed in table 2, the main part of the respondents were male (about three quarters). Our proportion of 25 percent of female CEOs is close to the 29 percent European figure (European Union, 2014).

Sizes of companies were distributed as follows: 58.8 percent micro-enterprises with less than ten employees, 29.4 percent businesses between 10 and 49 employees, and 11.9 percent of medium-sized businesses. Our sample shows a slight under representation of the smallest businesses compared to European figures (OECD, 2013), but remains closer than previous studies dedicated to information security in SMBs (Gupta and Hammond, 2004; Lee and Larsen, 2009).

The average age was around 40 years old (see Table 3).

Variable	**Frequency**	**Percent (%)**
Gender		
Male	132	74,6%
Female	45	25,4%
Size		
0-9	104	58,8%
10-49	52	29,4%
50-250	21	11,9%

Table 2: Demographic characteristics of the sample (N=177)

Table 3 shows the means, standard deviations, and correlations of our variables.

Variables	**Mean**	**SD**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1. Size	1,53	,70	1								
2. Gender	0,25	,43	,190*	1							
3. Age	39,9	12,08	-,132	-,087	1						
4. Vuln.	-,008	,99	-,068	-,047	**,196****	1					
5. Sev.	,007	,99	,002	,028	,047	,000	1				
6. Eff. R.	,008	,99	**-,230****	**-,151***	**,260****	,000	,000	1			
7. Eff. S.	,006	,99	**-,157***	-,139	-,095	,000	,000	,000	1		
8. Cost	,004	1	-,089	-,142	-,091	,000	,000	,000	,000	1	
9. Int	,007	,99	-,104	**-,162***	,066	**,224****	,058	**,298****	**,202****	**,199****	1

N= 177; Significance: *** p < 0.001; ** p < 0.01; * p<0.05

Table 3: Descriptive statistics and correlations

Table 4 presents the regression results. We integrated the control variables in Model 1 to determine their effects. Model 1 reports no significant effects: neither the firm size, gender nor CIO's age impact significantly the behavioral intention. In Model 2, to test all hypotheses, we included the different independent variables to examine to which degree they determine behavioral intention.

The results of the F-test ($F = 8.26$; $p < .001$) are significant. Hence, we can reject the null hypothesis, concluding that there is strong evidence that the expected values in the groups differ.

We also evaluated the reliability by examining the multicollinearity of measures to determine their variance inflation factor (VIF). All VIF were less than 2, therefore we can say that all indicators have an acceptable reliability.

Variables	**Model 1**	**VIF**	**Model 2**	**VIF**
Step 1: Controls				
Size	-,069	1.050	,002	1.131
Gender	-,136	1.040	,053	1.087
Age	,045	1.022	,027	1.163
Step 2: Main Effects				
Vuln.			,232***	1.056
Sev.			,056	1.005
Eff. R.			,292***	1.128
Eff. S.			,189**	1.057
Cost			,187**	1.039
R^2	,031		,222	
Adjusted R^2	,014		**,185**	
ΔR^2	,031		,191	
F	1,82		8,26***	

Significance: *** p < 0.001; ** p < 0.01; * p<0.05

Table 4: Multiple regression analysis: Dependent Variable = Behavioral Intention

CIO's behavioral intention is significantly influenced by perceived vulnerability, and by coping appraisal (response efficacy, self-efficacy and response cost).

As shown in Table 4 and as illustrated in Figure 2, the total explained variance is 18.5 percent.

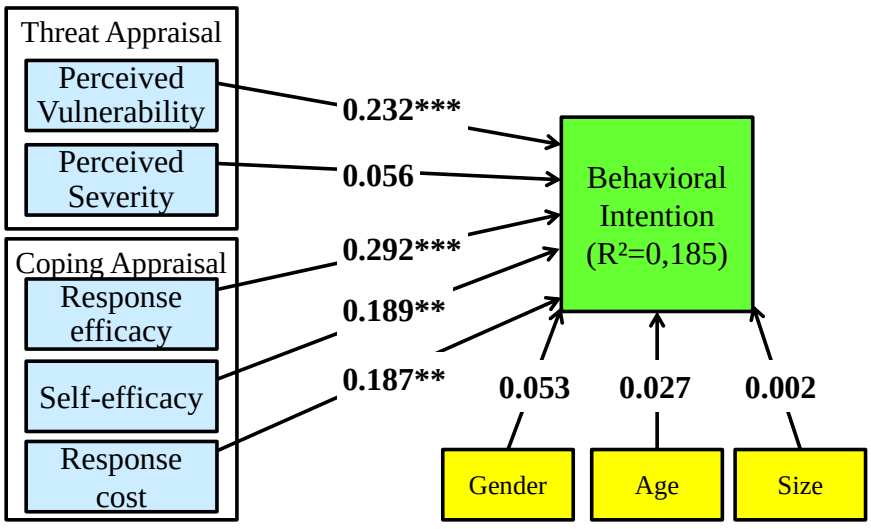

*Figure 2. Results for the tested hypotheses (***: p < 0.001; **: p < 0.01; *: p<0.05)*

Perceived vulnerability (β = 0.232; p < .001), Response efficacy (β = 0.292; p < .001) and Self-efficacy (β = 0.189; p < .01) serve as significant determinants of behavioral intention to implement security measures. These findings support hypotheses H1, H3 and H4.

Response cost (β = 0.187; p < .01) had an opposite influence contrary to what was expected, thus H5 is not supported.

The influence of Perceived severity was non-significant, thereby H2 is not supported.

None of our control variables, Gender, Age and Size showed any significant effect, therefore H6, H7 and H8 are not supported.

5. Discussion

Table 5 shows the previous studies we identified dealing with the Protection Motivation Theory.

Papers	**Year**	**Target Company size**	**Models tested**	**Behavioral Intention**	**Actual Behavior**
Workman et al.	2008	Employees Large IT firm	PMT (Threat control model)	N/A	**Take measure**s to protect infos (subjective) + logs (objective)
Herath & Rao	2009	Employees All Sizes	PMT, Deterrence	Compliance with Orga ISSP	N/A
Lee & Larsen	2009	**Executives SMB (2008)**	PMT, Social Influence	Support, encourage purchase	Purchases of antimalware soft
Ifinedo	2012	Employees All Sizes	PMT, TPB	Compliance with Orga ISSP	N/A
Vance et al.	2012	Administrative City Govt	Habit, PMT	Compliance with Orga ISSP	N/A
Yoon & Kim	2013	Employees All Sizes	PMT, TRA	**Take measures** to protect Info	N/A
Siponen et al.	2014	Employees All Sizes **(2006)**	PMT, TRA	Compliance with Orga ISSP	Compliance + Recommend & assist
Johnston et al.	2015	Employees City Govt	PMT, Deterrence	Changing Password	N/A

ISSP: I.S. Security Policy

Table 5: Previous studies and characteristics

If we compare our respondents with all the previous studies in table 5, only Lee and Larsen's study was dedicated to executives (yet nearly 60 percent were IS-experts) and to SMBs (yet less than 500 employees).

We posited that for the smallest sizes of businesses, as no CIO exists in the company, CEO's importance is reinforced in the management of information security.

Our study is clearly different from the previous ones because:

- SMBs of our sample follow the European definition: "Less than 250 employees", with an average size of 27 employees (vs. 192 employees for Lee and Larsen's study);
- We focused exclusively on CEOs ;
- Deterrence theory was not used because we contend that it is more relevant to explain employees' behavior than CEOs' one ;
- As 'behavioral intention', we used the implementation of IS security measures, as CEOs take part and/or support the creation and the implementation of security policies whereas compliance can be seen as more passive and more requested from employees.

Perceived vulnerability had a strong and significant positive influence on ISS behavioral intention. This confirms the results of Ryan (2004) and Bulgurcu et al. (2010) concerning CEOs. The more company's I.S. is perceived as vulnerable, the more CEOs tend to develop or apply ISS policies and procedures in their companies.

Response efficacy and self-efficacy had a positive influence on SMB CEOs' ISS behavioral intention: our study extends the results of Kankanhalli et al. (2003), showing that when CEOs have a positive perception of the efficacy of their behavior, they intend to be more secure and to implement ISS

measures. Our results are also in line with the results of Ifinedo (2012) and Lee and Larsen (2009) as we confirmed that behavioral intention is mainly influenced by coping appraisal.

Another interesting result is that if IS-experts accounted for nearly 60% of Lee and Larsen's study respondents (2009), 40 percent were non IS-experts (CEOs, CFOs and COOs[1]). They could assess strong differences between IS experts and non-IS experts. As very often CEOs are far from being IS experts, our results are also consistent with the fact that behavioral intention of non-IS experts is more influenced by coping appraisal, while behavioral intention of IS experts is more influenced by threat appraisal (Lee and Larsen, 2009, p. 184). Therefore, the fact that perceived severity had a weak and non-significant influence in our study is also in line with Lee & Larsen's findings.

The size of the company was not relevant to explain CEO's behavioral intention to take or implement security measures: this means that when the CEO is alone or even if a dedicated function exists (CIO or other employee who takes in charge information security), the CIO's level of intention to act doesn't vary significantly. Therefore, our study confirms the importance of CEOs' role in SMBs' ISS.

Surprisingly, response cost influenced positively the CEO's behavioral intention, which is counterintuitive and contradictory to previous studies results. Such result means that the more CEOs feel costly their behavior in terms of efforts or inconveniences, the more important their behavioral intention. We can suppose that CEOs feel that information security is not only important, but also implies vital and compulsory changes in their SMBs. Response cost could be, in this case, linked with the perception of ISS as a strategic issue and with the level of CEOs' commitment in their businesses. Studying the link between response cost, CEOs' commitment and the related stakes, would be an interesting avenue for future research.

To conclude with this discussion, in our study the strongest effect was exerted by response efficacy, explaining 30 percent of behavioral intention variance. Self-efficacy and response cost also proved to have a significant although lower effect.

5.1. Limitations

Although this study's findings provide meaningful implications, our study has some limitations.

First, our research used a web-based questionnaire, which may have introduced response bias because people outside the target population may fill out the questionnaire, or people in the target population could submit more than one response: even if we partially addressed this problem by controlling the respondent's IP address, by eliminating companies' sizes over 250 employees, some non-CEOs could have filled our questionnaire.

Second, this study only examined positive actions instead of maladaptive actions which may require further investigation.

Third, we could not assess the effects of certain variables such as industry type or the fact that a company is IT-intensive or not (Lee and Larsen, 2009).

To end, this study did not examine actual ISS-related behavior. It would be interesting to compare the behaviors of taking or implementing security measures in large companies (Workman et al., 2008) with actual behaviors in SMBs.

5.2. Implications for researchers and practitioners

This study confirmed the importance of CEOs' role in SMBs' ISS. SMB CEOs must realize that they sometimes just have to communicate on the importance of information security or set an example (such as shredding confidential documents), and security measures are not systematically expensive or cumbersome. As numerous meetings and seminars are organized for entrepreneurs, trainings or communications during those events could integrate some advice and insist on good practices related to ISS.

For researchers, we showed that even if it is relevant to study employees' behaviors - to decrease negative behaviors and improve positive behaviors - it is of utmost importance to dedicate more research on SMB CEOs as they constitute a specific and important population, and as it has been proved that their actions influence employees' behavior and have a strong impact on SMBs' overall security (Barlette, 2012).

[1] Chief X Officer. X = E for Executive, O for Operation, F for Finance.

6. Conclusion

The involvement of CEOs in implementing security measures is important for improving the level of information security in SMBs. We tested a model based on protection motivation theory (PMT) using data collected from 177 French SMB CEOs.

The results showed that response efficacy had the strongest effect, explaining 30 percent of behavioral intention variance. Self-efficacy and response cost also proved to have a positive and significant impact on CEOs' intention to implement information security measures. On the contrary, perceived vulnerability did not have a significant impact on the behavioral intention to implement these measures.

We highlighted some of the reasons why CEOs' ISS behavior was so important in SMBs in general and more particularly in the smallest ones where the CEO cannot rely on an internal IT expert.

It will be also interesting to identify actual actions, especially who takes ISS in charge in SMBs, and for which size of SMB. For example, we could identify thresholds were IT people or a CIO exist, or in the smallest SMBs, employees assuming this charge informally. This could be a trigger for CEO-specific behavior or at least provide insight on their ISS-related behavior.

The next step of this study will consist in working with a more important dataset, including social influence and other variables and the notion of direct (doing) and indirect behavior (supporting the person who does, when the CEO does not act).

References

Anderson, C.L. and Agarwal, R., (2010). "Practicing safe computing: a multimethod empirical examination of computer user security behavioral intentions", *MIS Quarterly*, Vol. 34, n°3, p. 613-643.

Anderson, E.E. and Choobineh J. (2008). Enterprise information security strategies, *Computers & Security*, n°27, p. 22-29.

Ashenden, D. (2008). "Information security management: A human challenge?", *Information security technical report*, n°13, p. 195-201.

Avolio, F.M. (2000). "Best practices in network security: as the networking landscape changes, so must the policies that govern its use. Don't be afraid of imperfection when it comes to developing those for your group." *Network Computing* Vol. 60, n°20, p. 60-72.

Bandura, A. (1994). *Self-efficacy*. In V.S. Ramachaudran (Ed.), Encyclopedia of human behavior, Vol. 4, p. 71-81, New York, NY: Academic Press.

Barlette, Y. (2012). "Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME", *Systèmes d'Information et Management*, Vol. 17, n°2, p. 115-149.

Boss, S.R., Kirsh, L.J., Angermeier, I., Shingler, R.A. and 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*, n°18, p. 151-164.

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

Bulgurcu, B., Cavusoglu, H. and 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.

Chu, A. M. Y. and Chau, P. Y. K. (2014). "Development and validation of instruments of information security deviant behavior", *Decision Support Systems*, Vol. 66, p. 93-101.

Dong, L. (2008). "Exploring the impact of top management support of enterprise systems implementations outcomes", *Business Process Management Journal*, Vol. 14, n°2, p. 204-218.

Dong, L., Neufeld, D. and Higgins, C. (2009). "Top management support of enterprise systems implementations", *Journal of Information technology*, n°24, p. 55-80.

Dutta, A. and McCrohan, K. (2002). "Management's role in information security in cyber economy". *California Management Review*, Vol. 45, n°1, p. 67-87.

European Commission, (2014), *Annual report on European SMEs 2013-2014*, EU publication office, 124p.

Forcht, K.A. and Ayers, W.C. (2000). "Developing a computer security policy for organizational use and implementation", *Journal of Computer Information Systems*, Vol. 41, n°2, p. 52-57.

Friend, M. and Pagliari, L.R. (2000). "Establishing a safety culture: getting started", *Professional Safety*, Vol. 45, n°5, p. 30-32.

Grover, V. (1993). "Empirically derived model for the adoption of customer-based inter-organizational systems", *Decision Sciences*, Vol. 24, n°3, p. 603-639.

Gupta, A. and 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.

Herath, T. and 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.

Hofstede, G., Neuijen, B., Daval-Ohayv, D. and Sanders, G. (1990). "Measuring organizational cultures: a qualitative and quantitative study

across twenty cases", *Administrative science quarterly*, Vol. 35, p. 286-316, Cornell university.

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, p. 83-95.

Jarvenpaa, S.L. and Ives, B. (1991). "Executive involvement and participation in the management of information technology". *MIS Quarterly*, Vol. 15, n°2, p. 205-227.

Johnston, A.C. and 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. and Siponen, M. (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.

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y. and Wei, K.-K. (2003). "An integrative study of information systems security effectiveness", *International Journal of Information Management*, n°23, p. 139-154.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R. and Nelson Ford, F. (2006). "Information security: management's effect on culture and policy". *Information Management and Computer Security*, Vol. 14, n°16, p. 24-36.

Kotulic, A. and Clark, J.G. (2004). "Why there aren't more information security research studies". I*nformation and Management*, Vol. 41, n°5, p. 597-607.

Kyobe, M. (2008). "The impact of entrepreneur behaviours on the quality of e-commerce security: A comparison of urban and rural findings", *Journal of global information technology management*, Vol. 11, n°2, p. 58-79.

Labodi, C. and 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.

Lazarus, R. S. (1991). *Emotion and adaptation*, Oxford University Press, NY.

Lee, Y. and 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, p. 177-187.

Liang, H. and Xue, Y. (2010). "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective", *Journal of the AIS*, Vol. 11, n°7, p. 394-413.

Longeon, R. and Archimbaud, J.L. (1999*). Guide de la sécurité des S.I. à l'usage des directeurs*, CNRS, Paris.

Loonam, J.A. and McDonagh, J. (2005). "Exploring Top Management Support for the introduction of Enterprise Information Systems: A Literature Review", *The Irish Journal of Management*, Vol. 26, n°1, p. 163-178.

Lucas, H.C. Jr. (1981). *Implementation: the key to successful information systems*, New York, NY: Columbia University Press.

Markus, M.L. (1983). "Power, politics, and MIS implementation", *Communications of the ACM*, Vol. 26, n°6, p. 430-444.

Mitchell, R.C., Marcella, R. and Baxter, G. (1999). "Corporate information security management". *New Library World* Vol. 100, n°1150, p. 213-227.

Monnoyer, M.C. (2003). *Le manager confronté à la décision d'investissement en TIC*, in Boutary, TIC et PME: des usages aux stratégies, Paris: l'Harmattan.

Pahnila, S., Siponen, M. and Mahmood, A. (2007). "Employees' behavior towards IS security policy compliance", *40th Hawaii International Conference on Systems Science (HICSS)*, January 3-6, IEEE, Los Alamitos.

Pinto, J.K. and Slevin, D.P. (1987). "Critical factors in successful project implementation". *IEEE Transactions on Engineering Management*, Vol. EM-34, n°1, p. 22-27.

Podsakoff, P.M., MacKenzie S.B., Lee J.Y. and Podsakoff NP. (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.

Pritchard, S. (2010). "Navigating the black hole of small business security", *Infosecurity*, Sept. Oct., p. 18-21.

Ragu-Nathan, B.S., Apigian, C.H., Ragu-Nathan, T.S. and Tu, Q. (2004). "A path analytic study of the effect of top management support for information systems performance", *Omega*, Vol. 32, p. 459-471.

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

Rees, J. (2010). "Information security for small and medium-sized business", *Computer Fraud & Security*, Vol. 9, p. 18-19.

Reid, R.C. and 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. and Volonino, L. (2004). *Principles and practices of information security*, Pearson Prentice Hall, New Jersey.

Rockart, J.F. and Crescenzi, A.D. (1984). "Engaging top management in information technology". *Sloan Management Review*, Vol. 25, n°4, p. 3-16.

Rogers, R. (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, NY, p. 153-176.

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

Ross, J. and Weill, P. (2002). "Six decisions your IT people shouldn't make", *Harvard Business Review*, November, p. 85-91.

Ryan, J. (2004). "Information security tools and practices: What works?", *IEEE Transactions on Computers*, n°53, p. 1060-1064.

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

Stemberger, M.I., Manfreda, A. and Kovacic, A. (2011). "Achieving top management support with business knowledge and role of IT/IS personnel", *International Journal of Information Management*, Vol. 31, p. 428-436.

Stevens, J.M., Beyer, J.M. and Trice, M.H. (1978). "Assessing personal role and organizational predictors of managerial commitment", *Academy of Management Journal*, n°21, p. 380-396.

Vance, A., Siponen, M. and Pahnila, S. (2012). "Motivating IS security compliance: Insights from habit and Protection Motivation Theory", *Information & Management*, Vol. 49, p. 190-198.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003). "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol. 27, n°3, p. 425-478.

Vermeulen, C. and von Solms, R. (2002). "The information security management toolbox: Taking the pain out of security management", *Information Management & Computer Security*, Vol. 10, n°3, p. 119-125.

Williams, P. (2007). "Executive and board roles in information security", *Network Security*, 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.

Workman, M., Bommer, W. H. and 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, p. 2799-2816.

Yoon, C. and Kim, H. (2013). "Understanding computer security behavioral intention in the workplace", *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.

Appendix A

	Variables	Authors	Item	Code
Coping Appraisal	Response efficacy	Adapted from Vance et al, 2012	Implementing information security policies in our organization keep IS security breaches down.	EFFR1
		Adapted from Vance et al, 2012	If I comply with information security policies, IS security breaches are scarce.	EFFR2
	Self-efficacy	Vance et al. 2012	I can implement information security policies by myself.	EFFS1
		Vance et al. 2012	Implementing information security policies is easy for me.	EFFS2
		Lent et al. 2006	I have the capability to solve possible problems during the implementation of security measures.	EFFS3
	Response cost	Vance et al, 2012	Complying with information security policies would require considerable investment of effort other than time.	COST1
		Vance et al, 2012	There are too many overheads associated with complying with information security policies.	COST2
		Vance et al, 2012	Complying with information security policies inconveniences my work.	COST3
Threat Appraisal	Perceived severity	Adapted from Vance et al, 2012	If I lost my computerized data, there would be serious information security problems for my organization.	SEV2
		Adapted from Vance et al, 2012	If my computerized data were temporarily not available, serious information security problems would result.	SEV3
	Perceived vulnerability	Vance et al, 2012	An information security problem could occur if I did not apply security policies.	VULN1
		Vance et al, 2012	I could be subjected to an information security threat, if I did not apply information security policies.	VULN2
		Vance et al, 2012	My organization could be subjected to an information security threat if I did not apply security policies.	VULN3
Behavioral intention		Adapted from Workman et al, 2008; Yoon and Kim, 2013	I intend to implement security measures in the next months.	INT1
			I plan to implement security measures in the next months.	INT2
Control Variables	Age	Venkatesh et al, 2003	Age	AGE
	Gender	Venkatesh et al, 2003	Male =0; Female =1	GEND
	Firm Size	European Union	<10 employees =1 ; 10-49 employees =2; 50-250 employees =3	SIZE

NB: The colors used for the variables are in line with those of our model.