European Journal of Information Systems (2009) 18, 177–187

www.palgrave-journals.com/ejis/

Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software

Younghwa Lee[1] and
Kai R. Larsen[2]

[1]School of Business, University of Kansas, Lawrence, KS 66045, U.S.A.; [2]Operations and Information Management Division, Leeds School of Business, University of Colorado at Boulder, Boulder, CO 80309, U.S.A.

Correspondence: Younghwa Lee, School of Business, University of Kansas, Lawrence, KS 66045, U.S.A.
Tel.: +785-864-7559;
Fax: +785-864-5328

Abstract
This study presents an empirical investigation of factors affecting small- and medium-sized business (SMB) executives' decision to adopt anti-malware software for their organizations. A research model was developed by adopting and expanding the protection motivation theory from health psychology, which has successfully been used to investigate the effect of threat and coping appraisal on protective actions. A questionnaire-based field survey with 239 U.S. SMB executives was conducted, and the data were analyzed using partial least squares (PLS). This study demonstrates that threat and coping appraisal successfully predict SMB executives' anti-malware software adoption intention, leading to SMB adoption. In addition, considerable variance in adoption intention and actual SMB adoption is addressed by social influence from key stakeholders and situation-specific variables, such as IT budget and vendor support. Further, the generalizability of the model was tested using industry type and IS expertise. The adoption intention of IS experts and IT intensive industries was mainly affected by threat appraisal and social influence, while that of non-IS experts and non-IT intensive industries was significantly influenced by coping appraisal and IT budget. Vendor support was a key facilitator of the anti-malware adoption for IS experts and IT intensive industry groups, while IT budget was for non-IS expert and non-IT intensive industry groups. Key implications for theory and practice are discussed.
European Journal of Information Systems (2009) **18,** 177–187. doi:10.1057/ejis.2009.11; published online 31 March 2009

Keywords: protection motivation; anti-malware; technology acceptance; partial least squares

Introduction

Understanding factor that influence the adoption of security systems is a topic of continuing interest (Straub & Welke, 1998; Lee & Kozar, 2005). Previous IS research on computer security has attempted to identify the reasons why individual users or employees adopt or do not adopt protective systems (e.g., Lee & LaRose, 2004). General IS acceptance theories including the Technology Acceptance Model, Theory of Planned Behavior, and Innovation Diffusion Theory have often been used as theoretical frameworks for addressing the adoption of protective systems (e.g., Hu & Dinev, 2005; Lee & Kozar, 2005), postulating that the factors affecting innovative information systems adoption can also successfully address protective systems adoption.

While such studies provide us with useful insights, deepening our understanding of factors and the decision-making process of protective

Received: 18 April 2008
Revised: 15 August 2008
2nd Revision: 27 January 2009
Accepted: 23 February 2009

systems adoption, uncharted terrains worthy of further exploration still exist. First, despite that security technologies are not intended to enhance productivity or to increase efficiencies in task completion, previous studies (e.g., Hu & Dinev, 2005; Chenoweth *et al*., 2007) have considered them as productivity-enhancing technologies (e.g., spreadsheets or email) and adopted generic IT adoption theories to address their adoption. Some key variables of the theories such as relative advantage, ease of use, as well as enjoyment thus cannot be applicable. Second, although a number of speculations have been made about the critical influence of perceived risk toward cyber attacks on personal or organizational protective systems adoption, there are few studies that scientifically validate the relationship. Limited attention to the threat has been considered a major reason why companies have not adopted protective systems, deferred the adoption, or adopted inappropriate systems (Willison & Backhouse, 2006). Finally, target subjects of previous studies on IS security were constrained to individual users or large-size enterprises, rather than SMBs. SMBs have unique characteristics differentiating them from large-sized enterprises, including centralized decision-making structures and lack of human and financial resources (Thong, 1999). In addition, because hackers prefer using SMB computing systems as decoys when attacking large-scale enterprise systems, SMB protective systems adoption is in need of separate attention.

This study explores these previously unexplored issues by examining the determinants affecting SMB executives' adoption of anti-malware software for their organizations by using the protection motivation theory (PMT) (Rogers, 1983). The PMT framework was chosen because it has been successfully applied in attempts to understand and predict a diverse array of protective actions (Milne *et al*., 2000). Instead of adopting the original PMT, this study attempts to expand the model by using the Structurational Model of Technology (Orlikowski, 1992), which explains the adoption of technology in organizations as the interplay among organizational properties, human agents, and technology. This study develops the extended PMT model by selecting situation-specific behavioral control variables and a social influence variable as organizational properties, PMT variables as human agents, and anti-malware software as the technology.

Research background

Previous studies on protective systems adoption

Research in the information systems security area can be divided into two streams based on the assumption about the role of individuals: individuals as potential abusers *vs* individuals as potential protectors (Lee & Lee, 2002). Researchers of the first research stream see employees or individuals as potential abusers and examine ways to deter or prevent their intention to breach personal or corporate computing systems. By adopting the general deterrence theory of criminology (Beccaria, 1963), which posits that the deviant behavior can be deterred if the potential abusers fear detection and prosecution, researchers (Straub & Welke, 1998) have found factors that effectively counteract employees' abusive actions. These researchers have proposed strong security policy enforcement, development and operation of security systems, and deployment of periodic security awareness programs as countermeasures which increase criminals' perception of the cost associated with computer abuse. However, those countermeasures do not lead to practical success because employees, who were treated as potential abusers in organizations, have resisted or only passively supported the implementation and operation of those countermeasures. For example, such employees do not actively participate in awareness programs.

Meanwhile, researchers in the second stream consider employees or individuals as potential protectors of their computing systems, and have focused on developing effective protective systems and identifying factors motivating consumer use of protective systems. For example, from the technology side, Cody *et al*. (2008) proposed systems security and behavioral security solutions for grid computing, and Zhao & Pechmann (2007) proposed a certification mechanism to align the incentives for service providers to protect their computer networks and customers. However, compared to the many studies which propose security systems solutions and test their functional efficiency and effectiveness, only a few studies (e.g., Hu & Dinev, 2005; Lee & Kozar, 2005) have examined human-side behavioral solutions that can effectively motivate the individual adoption of security solutions. Furthermore, the behavioral solution studies have been based on generic IS adoption theories, and have only investigated the effectiveness (e.g., relative advantage) and efficiency factors (e.g., ease of use), without examining the threat factors.

Protection motivation theory

PMT (Rogers, 1983) has been a valuable theoretical framework in health and social psychology, providing an important social cognitive account of a variety of protective behaviors. PMT as an expectancy-value theory addresses the tendency to engage in protective behavior as a function of the expectancy that the behavior will be followed by certain consequences and the value of those consequences. The basic postulate of this theory is that protection motivation arises from the cognitive appraisal of a threatening event as serious and likely to occur, together with the belief that a recommended coping response can effectively prevent its occurrence (Milne *et al*., 2000). The threat appraisal is associated with threats (or danger) of continuous maladaptive response. The likelihood of an adaptive response is increased when perceptions of severity and vulnerability are high, while it is reduced when any rewards associated with continuing the maladaptive response are expected (McMath & Prentice-Dunn, 2005). The coping appraisal is associated with proposed adaptive recommendations, and evaluates

one's ability to cope with and avert the threatening behavior. It is related to the individual's assessment of the effectiveness of the proposed adaptive behavior to avert the threat (i.e., response efficacy) and the perceived ability to conduct the advocated behavior (i.e., self-efficacy). The likelihood of enacting the adaptive behavior is increased when high levels of the efficacy variables are predicted. Meanwhile, the likelihood is decreased when high response costs associated with performing the adaptive behavior are perceived. Essentially, the combination of the threat appraisal and coping appraisal processes activates a person's protective motivation, resulting in the applicable adaptive responses. PMT has been validated in various non-technology settings such as breast self-examinations (Fry & Prentice-Dunn, 2005), natural disaster precautionary action (Grothmann & Reusswig, 2006), and anti-smoking programs (Pechmann *et al.*, 2003).

Hypotheses development

Assuming that the decision of SMB executives to adopt anti-malware software for their organizations is strongly influenced by both threat and coping appraisals, this study proposes and develops a theoretical model (see Figure 1) by adopting and extending PMT. The research hypotheses, major variables, and their definitions are summarized in Table 1.

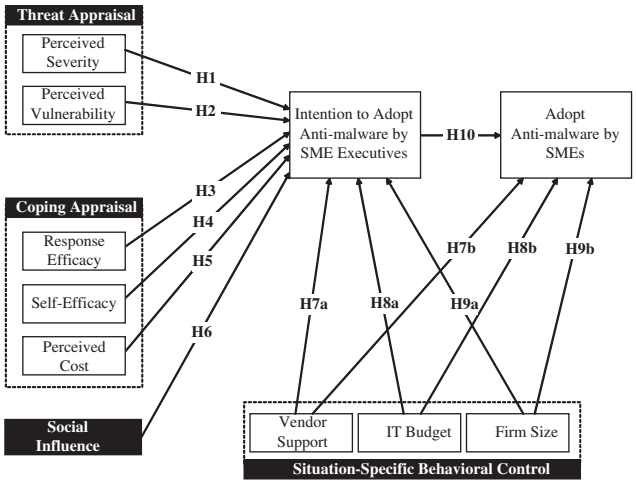

Figure 1 Research model.

Table 1 Summary of research hypotheses, major variables, and their definitions

Variable	*Definition*	*Hypothesis*
Perceived severity	The degree of physical harm, psychological harm, social threats, economic harm, dangers to others rather than oneself, and even threats to other species	H1: Perceived severity positively influences SMB executives' intention to adopt anti-malware software for their organizations
Perceived vulnerability	The conditional probability that the threatening event will occur provided that no adaptive behavior is performed or there is no modification of an existing behavioral disposition	H2: Perceived vulnerability positively influences SMB executives' intention to adopt anti-malware software for their companies
Response efficacy	The belief that the adaptive response will work in averting an undesirable threat	H3: Response efficacy positively influences SMB executives' intention to adopt anti-malware software for their organizations
Self-efficacy	The belief that one is or is not capable of performing a coping behavior	H4: Self-efficacy positively influences SMB executives' intention to adopt anti-malware software for their organizations
Response cost	Any costs (e.g., monetary, time, effort, inconvenience, unpleasantness, difficulty, complexity, side effects) associated with taking the adaptive coping response	H5: Response cost negatively influences SMB executives' intention to adopt anti-malware software for their organizations
Social influence	The pressure to perform or not perform a behavior that is determined by a person's inclination to comply with people who are important to him or her	H6: Social pressure from referents associated with adopting anti-malware software significantly influences SMB executives' intention to adopt the systems for their organizations
Vendor support	Services provided by software vendors	H7: Vendor support positively affects SMB executives' intention to adopt anti-malware software (H7a) and actual adoption (H7b)
IT budget	Annual IT budget of SMBs	H8: Annual IT budget of SMBs influences their executives' intention to adopt anti-malware software (H8a) and actual adoption (H8b)
Firm size	Firm size of the SMBs	H9: Firm size positively affects SMB executives' intention to adopt anti-malware software (H9a) and actual adoption (H9b)
Adoption intention	An indication of a person's readiness to perform a given behavior	H10: SMB executives' intention to adopt anti-malware software is positively related to actual SMB adoption

The perceived severity (H1) exerts a significant effect on the intentions to follow protective actions (Pechmann *et al.*, 2003). It is expected that the more seriously a person perceives the magnitude of the negative consequences resulting from continuing maladaptive actions, the more he adopts recommended adaptive actions. Similarly, we expect that SMB executives perceive malware as a severe threat for their enterprise computing systems. Malware is a 'sophisticated malicious program designed to move from computer to computer and network to network to intentionally modify computer systems without the consent of the owner and operator' (Grimes, 2001). It has evolved as a serious danger for computer users and is, at present, considered the most common and dangerous source of cyber attacks (Etsebeth, 2007). Using sophisticated hiding technologies such as stealth and self-mutating methods, malware can hide itself before, during, and after it infects target systems. Malware can ensconce itself until users access specific files or websites and pilfer user ID, passwords, and data, and then delete all footprints on the infected systems. Malware writers continuously produce more advanced forms of malicious code such as FormSpy, RFID malware, and Bluetooth malware. Given these threats, SMB executives are expected to intend to adopt anti-malware software for their organizations.

The perception of vulnerability (H2) is associated with an individual's assessment of his/her probability of being exposed to the unfavorable threat. Thereby, the likelihood of adopting the advocated adaptive behavior is increased when a person perceives high vulnerability. Previous studies have found the variable's significant effect on the intentions to adopt protective behaviors (McClendon & Prentice-Dunn, 2001). Along the same vein, SMB executives are expected to seriously consider the adoption of anti-malware software for their organizations when they perceive that their organizations have a high likelihood of being exploited by malware attacks.

Given the information about the counteractive measures for coping with the threats, a person assesses the efficacies of the advocated adaptive behavior (H3). Anti-malware software has been reported as an effective and efficient tool for detecting and deterring malware attacks. By implementing a variety of detection algorithms and techniques such as code optimization and semantic-aware signatures, a variety of anti-malware software including ClamAV, BOClean, AVG anti-malware, and Rootkit Detective have been developed. Furthermore, their effectiveness to detect and remove malware has been empirically validated (Bruschi *et al.*, 2007). Because the higher the individual perceives a response efficacy, the greater likelihood of enacting the adaptive behavior is predicted, response efficacy should positively influence SMB executives intention to adopt anti-malware software.

Self-efficacy (H4) has been found to have a robust effect on intentions to perform protective actions (Milne *et al.*, 2000). If people have high confidence in their ability to conduct a recommended action, and they feel the action is not difficult, they are more likely to adopt the action (Bandura, 1977). The significant effect of self-efficacy on the intentions of protective actions has been found in various behavioral contexts (McClendon & Prentice-Dunn, 2001; Pechmann *et al.*, 2003). In the team or organizational context, individual-focused self-efficacy has evolved to measure the belief on the aggregated capabilities of team or organizational members as collective self-efficacy, often assessed by team leaders or organizational representatives (e.g., Bandura *et al.*, 1999). In organizational IT adoption studies (e.g., Chau & Tam, 1997), top managers were identified as individuals who can adequately assess the cumulative perceptions and capabilities of their organizational members associated with new IT adoption. Thus, this study predicts that the more SMB executives are convinced about their organizations' capability to learn, implement, and use anti-malware software, the stronger their intention to adopt anti-malware software for their organizations.

Individuals hesitate to adopt the recommended response if they have to dedicate a considerable amount of time, effort, and money, or feel awkward in conducting the effort (Milne *et al.*, 2000). Previous studies have found a significant negative impact of response cost (H5) on adaptive behaviors (Helmes, 2002). Examples of response cost are: the effort required to protect from skin cancer (Mcclendon & Prentice-Dunn, 2001), the frequent changes of the encryption key (Lee & Larose, 2004), and the discomfort in examining skin cancer (McClendon & Prentice-Dunn, 2001). The same negative effect is expected to be found in anti-malware software adoption. That is, SMB executives are less likely to adopt anti-malware software when they perceive high cost to adopt and operate the software and the significant performance decline of extant computer systems or networks.

PMT is a theoretical framework addressing a social cognitive account of protective behavior, but previous studies adopting PMT have mainly focused on a cognitive account, not a social account. Considering the strong influence of social factors (H6) on adopting IT (e.g., Venkatesh *et al.*, 2003), in particular, newly introduced technologies such as anti-malware software, it is valuable to include these factors in the PMT model and examine their effect on adopting security technologies. We expect that SMB executives are more likely to adopt anti-malware software for their organizations if they find that their business referents, including customers, business partners, community, and competitors, tend to adopt the software.

The significant effects of situation-specific control variables have been found in previous studies (e.g., Beck & Ajzen, 1991; Lee & Kozar, 2005). These variables have been considered as behavioral control variables which can strongly affect behavioral intention and actual behavior. In line with previous studies, we identified three situation-specific variables by conducting extensive interviews with SMB executives and examined their

influences on anti-malware software adoption and actual adoption. The control variables elicited through the interviews include vendor support (H7ab), IT budget (H8ab), and organizational size (H9ab). The limited number of internal IT experts available to support system implementation and operations in SMBs has been found to be a major inhibitor of the advanced systems adoption, leading many SMBs to take a passive stance on systems adoption. As one of the solutions to resolve this lack of human resources, previous SMB IT adoption studies have suggested the solicitation of extensive vendor support including the presence of designated technicians, easy access to technical assistance, and periodic training. The more vendor support is expected, the more SMB executives are inclined to adopt anti-malware software. An effect on the availability of resources, especially financial, on IT adoption has also been found. For example, Iacovou *et al*. (1995) cited the availability of financial resources as one of the important factors for the adoption of electronic data interchange (EDI) in small firms. Along the same vein, SMB executives with larger IT budgets are more likely to adopt the anti-malware software for their organizations. Finally, there has been research which investigates the impact of organizational size on technology adoption. For example, Forman (2005) found that organizational size has significant impact on the adoption of Internet applications. Researchers have also found that SMB size is positively related to adoption of technological innovations (Thong, 1999). Similarly, we expect that the larger an SMB is, the more likely the SMB can afford anti-malware software, resulting in its adoption.

The significant relationship between behavioral intention and actual behavior (H10) has been validated in both individual and organizational systems adoption contexts (e.g., DeLone & McLean, 2003). As with previous studies, this study predicts that when SMB executives intend to adopt anti-malware software, they are more inclined to purchase the software, leading to organizational adoption.

Research methodology

To validate measurement instruments for the proposed theoretical model and to investigate nomological networks between endogenous and exogenous variables, a questionnaire-based field survey was conducted with 239 SMB executives in the U.S. We selected the survey methodology because: (1) it minimizes the subjectivity of the research findings by gathering a large number of subjects and by employing statistical tests in data analysis and (2) it allows researchers to develop reliable measures for replicating the study in various contexts and comparing the findings of the study with those of existing models. The survey methodology is also convenient in reaching busy executives who work at geographically dispersed organizations. The survey method has been applied to many IS adoption studies (e.g., Chau & Tam, 1997). The data were analyzed using partial least squares (PLS) analysis, a latent structural equation modeling technique that has the capacity to estimate simultaneously both the structural model and the measurement model. We selected PLS because: (1) it can be used to examine a model that includes both formative and reflective indicators and (2) it places minimal demands on sample size, measurement scales, and residual distributions (Chin, 1998).

Consistent with previous studies on SMB (Riemenschneider *et al*., 2003), this study defined SMB as firms with less than 500 employees. Subjects were drawn from a database of current or potential SMB adopters of anti-malware software, and the executives were identified by the anti-malware software vendor. The list contains more than 1000 executives of 600 U.S. SMB organizations. An e-mail containing the invitation letter and online questionnaire was sent to the executives. The invitation included the description of malware, malware attacks, and anti-malware software to help the executives gain a better understanding of the context and terminology of the study.

A total of 275 responses were returned. After removing 36 incomplete and invalid responses, the remaining 239 usable responses were included in the data analysis. The overall response rate was 24%. One hundred forty-one subjects were IT executives while the rest were non-IT executives including CEO, chief financial officer, and chief operations officer. The respondents represented a number of different industries including manufacturing (37), professional (33), retail trade (17), construction (15), education services (17), finance (26), government (14), healthcare (19), and others. The average number of employees and PCs per company was 192.3 and 138.8 respectively. Companies spent an average of $4640 dollars on purchasing or updating anti-malware software.

Instruments were developed using scientific instrument development processes suggested by Straub (1989). The instrument items were developed through an extensive literature review on PMT, SMB IT adoption, and the theory of planned behavior. Concurrently, extensive interviews as in previous studies (e.g., Beck & Ajzen, 1991) were conducted with 11 executives to understand and gain insights into their companies' anti-malware software adoption. The instrument items were then operationalized to fit into the context of anti-malware software adoption and pretested with five experts who were familiar with PMT, SMB IS adoption, and instrument development. Through this process, the wording, order of items, content, and format of the questionnaire were revised. Seven-point Likert-type scales were used to measure those constructs. Table A1 shows the instrument items.

Results

Measurement model analysis: reflective indicators

Measurement model analysis was conducted to examine psychometric properties of the measures for reflective

Table 2 Inter-construct correlations and AVE along the diagonal

	CR	*Cronbach α*	*RE*	*SE*	*VEN*	*INT*
Response efficacy (RE)	0.898	0.857	**0.863**			
Self-efficacy (SE)	0.883	0.858	0.453	**0.846**		
Vender support (VEN)	0.898	0.829	0.347	0.307	**0.864**	
Adoption intention (INT)	0.925	0.858	0.636	0.450	0.408	**0.928**

Values shown in the main diagonal represent the square root of AVE.

constructs such as response efficacy, self-efficacy, vendor support, and adoption intention. Testing was done by examining convergent validity and discriminant validity. Convergent and discriminant validity can be assessed by applying two criteria: (1) the square root of the average variance extracted (AVE) by a construct from its indicators should be at least 0.707 (i.e., AVE$>$0.5) and should be greater than the variance shared between the construct and other constructs in the model, and (2) standardized item loadings should be at least 0.707, and no measurement item should load more highly on other constructs than the construct it intends to measure (Fornell & Larcker, 1981). As shown in Tables 2 and 3, convergent and discriminant validity was confirmed. The square root of AVE for each construct was greater than 0.707, and all constructs share more variance with their own indicators than with those of other constructs. In addition, the factor structure matrix shows that all indicators exhibited high loadings on their own constructs, and no items loaded higher on the constructs that they were not intended to measure.

Table 3 Factor structure matrix of loadings and cross-loadings

Indicator	*RE*	*SE*	*VEN*	*INT*
RE1	**0.851**	0.355	0.279	0.450
RE2	**0.902**	0.416	0.365	0.621
RE3	**0.890**	0.426	0.281	0.616
SE1	0.454	**0.908**	0.270	0.432
SE2	0.358	**0.878**	0.215	0.417
SE3	0.395	**0.860**	0.338	0.342
VEN1	0.293	0.231	**0.853**	0.309
VEN2	0.270	0.252	**0.880**	0.375
VEN3	0.351	0.304	**0.855**	0.376
INT1	0.616	0.448	0.373	**0.937**
INT2	0.598	0.401	0.399	**0.935**

Table 4 Validity and reliability test results of formative constructs

Construct	*Items*	*Weight*	*Standard error*	*T-value*	*VIF*
Perceived severity (PS)	PS1	0.204	0.102	1.998	2.683
	PS2	0.277	0.138	2.013	3.054
	PS3	0.352	0.148	2.384	2.763
	PS4	0.316	0.131	2.408	2.129
Perceived vulnerability (PV)	PV1	0.388	0.159	2.442	2.639
	PV2	0.361	0.133	2.720	2.659
	PV3	0.358	0.162	2.209	3.191
Response efficacy (RC)	RC1	0.379	0.180	2.101	2.721
	RC2	0.213	0.232	0.918	3.883[a]
	RC3	0.502	0.234	2.148	2.855
Social influence (SI)	SI1	0.460	0.206	2.236	2.488
	SI2	0.303	0.228	1.331	2.295
	SI3	0.363	0.168	2.159	2.326

[a]Removed from final data analysis because of high multicollinearity problem.

Measurement model analysis: formative indicators

Because of the nature of formative constructs, different analyses with reflective constructs need to be conducted to assess their validity and reliability. This study conducted measurement model analysis for four formative constructs such as perceived severity, vulnerability, response cost, and social influence following the guidelines proposed by Petter *et al*. (2007). First, we assessed construct validity by conducting a principal component analysis to examine the item weights for measures. As shown in Table 4, the results demonstrated the weights of all measurement items except those of two items (RC2 and SI2) were significant. In this study, we retained those insignificant items which were believed to be theoretically necessary for construct completeness. Previous studies (e.g., Marakas *et al*., 2007; Straub *et al*., 2008) also retained the insignificant items for the same reason. Second, we evaluated the reliability by examining the multicollinearity of measures to determine if their variance inflation factor (VIF) is less than 3.33 (Petter *et al*., 2007). The results showed that all items of formative constructs, except one item corresponding to response cost, had less than 3.33 VIF values. After removing the item, we found that all formative indicators had an acceptable reliability.

Structural model analysis

The structural model was tested by examining the path coefficients. In a PLS structural model, paths can be interpreted as standardized betas, and hence the explained variance in the endogenous variables is assessed as an indication of the overall predictive strength of the model. Following Wold (1982), a bootstrapping test was conducted to find estimates of standard errors for testing the statistical significance of path coefficients using *t*-tests. A total of 67% of the total variance of the

Table 5 Tests of hypotheses

Hypotheses	*Path coefficients*	*t-value*
H1: Perceived severity → Intention	0.252	4.096***
H2: Perceived vulnerability → Intention	0.120	2.389*
H3: Response efficacy → Intention	0.215	4.752***
H4: Self-efficacy → Intention	0.114	2.292*
H5: Response cost → Intention	−0.257	7.080***
H6: Social influence → Intention	0.121	2.418**
H7a: Vendor support → Intention	0.074	2.320*
H7b: Vendor support → Adoption	0.145	1.986*
H8a: IT budget → Intention	0.139	3.280**
H8b: IT Budget → Adoption	0.139	2.191*
H9a: Firm size → Intention	0.020	0.495
H9b: Firm size → Adoption	0.081	1.409
H10: Intention → Adoption	0.337	5.678***

*$P<0.05$, **$P<0.01$, ***$P<0.001$, R^2 for the Adoption Intention = 0.696, and R^2 for the Adoption = 0.262.

intention to adopt anti-malware software and 26.2% of that of the actual adoption were explained. Table 5 shows the path loadings for all hypothesized relationships. SMB adoption was significantly influenced by executives' adoption intention, vendor support and IT budget, not by firm size. All threat appraisal, cognitive appraisal and social influence variables, in addition to vendor support and IT budget, showed a significant influence on adoption intention.

Multi-group analysis

To test the generalizability of the model, we conducted multi-group analyses by dividing the subjects by the industry type (IT intensive *vs* non-IT intensive) and IS expertise (IS expert *vs* non-IS expert). Using two measures such as the primary industry type (e.g., finance is classified into IT intensive, and construction is non-IT intensive) and annual IT budget as a percentage of the annual corporate budget, we classified each SMB as IT-intensive ($n=114$) or non-IT intensive ($n=125$). Executives' IS expertise was measured using four items, including individual's PC use experience, Internet experience, computer proficiency, and position (e.g., IS managers), resulting in 143 IS-experts and 96 non-IS experts. After conducting multi-group analyses, we found that model constructs explained a large amount of variance of anti-malware software adoption intention (at least 65.4%) and adoption (at least 24.5%). As shown in Figure 2, several interesting differences between different groups with respect to the strength of the relationships between threat appraisal, coping appraisal, social influence, and the adoption were found.

Following the marker variable (MV) technique of Malhotra *et al*. (2006), this study examined the common method bias. We used social desirability as an MV which is theoretically unrelated to at least one variable in the study. Because the market variable is presumed to have no relationship with one or more variables in the study, CMV can be assessed based on the correlation between the market variable and the theoretically unrelated variable. Three items with a high reliability (Cronbach $\alpha=0.818$) were used to measure social desirabilitiy. We first conducted a correlation analysis to find the value of an MV, which were used as an indicator of common method bias, and found that it was 0.014. Then, by putting it into the formula provided by Malhotra *et al*. (see p. 1868), we created adjusted correlation estimates and *t*-statistics. As a result, we found that none of the original correlations were significantly different from their CMV-adjusted counterparts, implying that the biases are not substantial.

Discussion and implications

By adopting the PMT in health psychology and expanding it to include social influence and situation-specific control factors, this study proposed and validated a research model to investigate the factors affecting SMB executives' anti-malware software adoption. The results show that a significant amount of variance in SMB software adoption was explained by the model. All threat appraisal and coping appraisal variables were found to significantly affect SMB executives' anti-malware software adoption intention. This implies that SMB executives' adoption decision is influenced by both the magnitude of negative consequences from malware attacks and organizational vulnerability to the attacks, as well as the capability to counteract the attacks and the expected costs and efficacies associated with adopting the countermeasures.

Both perceived severity and vulnerability were found to significantly influence the intention to adopt anti-malware software. Perceived severity was the most influential factor, indicating that the degree of expected harm from malware attacks is the strongest motivator of the software adoption. The influence of perceived vulnerability was also significant, but its effect was relatively weaker than expected. However, this does not mean that we have to treat vulnerability as less important – the effect of vulnerability might not be fully captured because executives may be overconfident on the capability of existing security systems to detect or remove malware. Providing free vulnerability tests and test result reports to SMB executives can help increase their awareness. The finding of the significant effect of threat appraisal indicated that threat received a lack of attention in previous studies and should be considered in future studies on protective systems adoption.

Coping appraisal variables were also found to significantly affect anti-malware software adoption. Response efficacy was the strong facilitator of the adoption intention, indicating that SMB executives are highly motivated to adopt the software when they predict high expected returns of adopting the recommended protective systems. The significant effect of self-efficacy represents that SMB executives are willing to adopt the software when they are confident in their organizations' ability to adopt and operate it. Finally, there was a

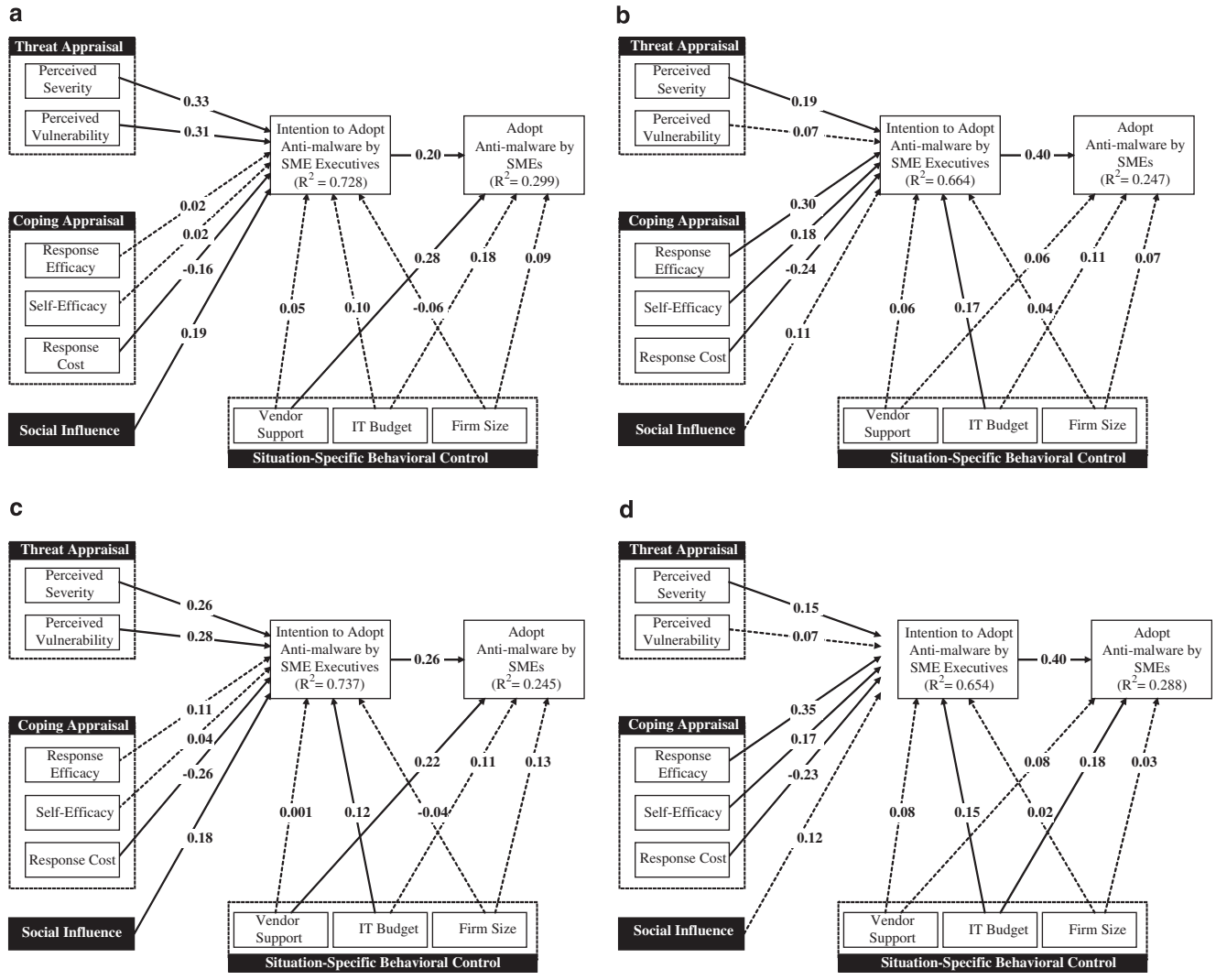

Figure 2 Results of multi group analyses. (a) IS expert; (b) Non IS-expert; (c) IT intensive industry; (d) Non-IT intensive industry.

significant negative influence of response cost on adoption intention. It indicates that developing different versions of anti-malware software to meet the system requirements of SMB computing systems, specifically so as not to deteriorate the systems' performance, will help reduce the executives' concerns around software adoption. These findings of coping appraisal confirmed that traditional socio-economic models still work effectively in the context of anti-malware software adoption.

Interestingly, this study demonstrated that the effect of threat and coping appraisal on the adoption decision was strongly influenced by executives' IS expertise and industry type. As shown in Figure 2, for the IS expertise, the adoption intention of the IS experts was mainly influenced by threat appraisal, while that of non-IS experts was mainly influenced by coping appraisal. Adoption intention and vendor support were two key variables of the actual adoption by the IS experts, while adoption intention was the only significant variable affecting adoption by non-IS experts. Similarly, threat appraisal was dominant over coping appraisal for the adoption intention of the IT intensive industries, while coping appraisal was dominant for non-IT intensive industries. Actual adoption by IT intensive industries was mainly influenced by adoption intention and vendor support, while that of the non-IT intensive industries was influenced by adoption intention and IT budget. The finding provides vendors with useful insights into developing effective marketing efforts. By identifying target executives' IS expertise and industry type, vendors can develop customized advertisement portfolios to attract SMB executives more effectively.

Significant social influence was also found in this study. This implies that executives seriously consider others' perceptions toward anti-malware software adoption before adopting the software. That is, in SMB

business environments, where barriers to entry are low and the competition is fierce, SMB executives carefully attended to the preference of their stakeholders including customers, business partners, and even competitors toward the systems adoption. In particular, the fact that social influence was significant for IT intensive industry and IT expert groups, while it was not for non-IT intensive industry and non-IS expert groups, implies that SMBs that are IT-knowledgeable and IT-dependent are more sensitive to the opinions of their referents in the context of anti-malware software intention to adopt or actual adoption. As predicted, vendor support and IT budget significantly affected the adoption intention and actual adoption . It implies that the provision of attractive vendor support, including local presence, 24×7 services, on-site training, user-friendly online and paper-based user and operator manuals, in addition to the provision of an affordable system will be crucial in persuading executives to adopt the software. Finally, this study found that firm size did not show a significant effect on the adoption intention and actual adoption, while IT budgets showed a significant effect. This is contrary to our expectation since previous studies have found that the larger a firm is the bigger investment it made on purchasing IS. The finding can be interpreted based on the low correlation between IT budget and firm size (Pearson correlation = 0.186). That is, at least in the context of this study, it is not a valid statement that the larger firm has the larger IT budget.

This study does have limitations that should be revisited in the future. First, although we conducted a common method bias test and confirmed no significant self-selection bias present, objective adoption data should be gathered to avoid self-selection bias in future studies. Second, this study did not compare the present model with previous IT adoption models and test it in alternative organizational contexts, such as in large enterprises. This should be performed in future studies. Third, this study only examined (positive) adaptive actions instead of examining diverse maladaptive actions, which will require further investigation. Fourth, this study did not examine the impetus to PMT variables, assuming that subjects are fully aware of threat from malware attacks and effectiveness of anti-malware software to counteract it. Controlled experiments are recommended to better understand the influence of different kinds of impetus. Finally, because of the sample size limitation, we did not fully examine the effects of SMB characteristic variables, including industry type. It is recommended for future studies to carefully sample SMB executives to examine the effect of those SMB specific variables.

This study provides several useful implications for both researchers and practitioners. From a researcher's perspective, this study proposes and validates a theoretical model by adopting PMT to identify factors affecting the adoption of protective software by considering threat appraisal variables, which have not been investigated before. In addition, this study successfully demonstrates that the expanded model with social influence and situation-specific control variables explains a significant amount of variance of the anti-malware software adoption. It suggests that the model expansion by incorporating social influence and control factors was valuable exploration. The stability of the model was also tested and validated under different boundary conditions, such as industry type and IS expertise, indicating that the expanded model can be applied to address protective actions in various behavioral contexts. Further, this study enriches our understanding of SMB protective systems adoption by examining the relationship between executives' intention and organizational adoption.

From a practitioner's perspective, this study provides several useful insights for vendors of anti-malware software. On the basis of the findings of this study, vendors can prepare enlightenment programs or materials that address both the risk of malware attacks and the efficiency of anti-malware software. In addition, the findings provide useful information on developing the software and creating an effective marketing strategy. Some valuable guidelines include developing multiple versions to fit each SMB's various system configurations (e.g., consuming different amounts of computer memory) and IT budget, and customizing marketing campaigns based on executives' IS expertise and industry type to persuade them more effectively.

To summarize, by adopting and expanding the PMT, this study identifies factors motivating or inhibiting SMB executives' anti-malware software adoption for their organizations, allowing improvements to ongoing strategic efforts to increase software adoption.

Acknowledgements

The authors gratefully acknowledge grant support from Webroot Inc.

About the authors

Younghwa Lee is an Assistant Professor of information systems in the University of Kansas School of Business, Lawrence, KS, USA. He received his Ph.D. from University of Colorado at Boulder, Boulder, CO, USA, in 2005. His research interest is in technology acceptance, website usability, and IT ethics and security. He is an ICIS 2003 Doctoral Consortium fellow. He has published in *Communications of the ACM*, *Decision Support Systems*, *Information & Management*, *Journal of Organizational Computing and Electronic Commerce*, among others.

Kai R. Larsen is an Associate Professor of information systems in the University of Colorado at Boulder, Leeds School of Business, Boulder, CO, U.S.A. His research interests center around interdisciplinary approaches to information systems implementation, inter-organizational networks, and development and application of the automatic text analysis in IS research. He has published in *Journal of Management Information Systems*, *European Journal of Information Systems*, *Sociological Methodology*, and *Communications of the ACM* among others.

References

ADDIS M (2003) Basic skills and small business competitiveness: some conceptual considerations. *Education + Training* **43(3),** 152–161.

BANDURA A (1977) Self efficacy: toward a unifying theory of behavioral change. *Psychological Review* **84,** 191–215.

BANDURA A, FREEMAN WH and LIGHTSEY R (1999) Self-efficacy: the exercise of control. *Journal of Cognitive Psychotherapy* **13(2),** 158–166.

BECCARIA C (1963) *On Crime and Punishments*. Bobbs Merril, Indianapolis, IN.

BECK L and AJZEN I (1991) Predicting dishonest actions using the theory of planned behavior. *Journal of Research in Personality* **25,** 285–301.

BRUSCHI D, MARTIGNONI L and MONGA M (2007) Code normalization for self-mutating malware. *IEEE Security & Privacy* **5(2),** 46–54.

CHAU PYK and TAM KY (1997) Factors affecting the adoption of open systems: an exploratory study. *MIS Quarterly* **21(1),** 1–24.

CHENOWETH T, MINCH R and TABOR S (2007) Expanding views of technology acceptance: seeking factors explaining security control adoption. *AMCIS 2007 Proceedings* 321–328.

CHIN WW (1998) *The Partial Least Squares Approach to Structural Equation Modeling*. Lawrence Erlbaum Associates Mahwah, NJ.

CODY E, SHARMAN R, RAO RH and UPADHYAYA S (2008) Security in grid computing: a review and synthesis. *Decision Support Systems* **44(4),** 749–764.

DELONE WH and MCLEAN ER (2003) The Delone and Mclean model of information systems success: a ten-year update. *Journal of Management Information Systems* **19,** 9–30.

ETSEBETH V (2007) Malware: the new legal risk. *The Electronic Library* **25(5),** 534–542.

FORMAN C (2005) The corporate digital divide: determinants of internet adoption. *Management Science* **51(4),** 641–654.

FORNELL C and LARCKER DF (1981) Evaluating structural equations models with unobservable variables and measurement error. *Journal of Marketing Research* **18(1),** 39–50.

FRY RB and PRENTICE-DUNN S (2005) Effects of coping information and value affirmation on responses to a perceived health threat. *Health Communication* **17,** 133–147.

GRIMES RA (2001) *Malicious Mobile Code: Virus Protection for Windows*. O'Reilly & Associates, Inc., Sebastopol, CA.

GROTHMANN T and REUSSWIG F (2006) People at risk of flooding: why some residents take precautionary action while others do not. *Natural Hazards* **38,** 101–120.

HELMES AW (2002) Application of the protection motivation theory to genetic testing for breast cancer risk. *Preventive Medicine* **35,** 453–462.

HO R (2000) Predicting intention for protective health behaviour: a test of the protection versus the ordered protection motivation model. *Australian Journal of Psychology* **52(2),** 110–118.

HU Q and DINEV T (2005) Is spyware an internet nuisance or public menace? *Communications of the ACM* **48(8),** 61–66.

IACOVOU CL, BENBASAT I and DEXTER AS (1995) Electronic data interchange and small organizations: adoption and impact of technology. *MIS Quarterly* **19(4),** 465–485.

KAMBIL A, KALIS A, KOUFARIS M and LUCAS HC (2000) Influences on the corporate adoption of web technology. *Communications of the ACM* **43(11),** 264–271.

LEE Y and KOZAR KA (2005) Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM* **48(3),** 72–78.

LEE J and LEE Y (2002) A holistic model of computer abuse. *Information Management & Computer Security* **10(2),** 57–63.

LEE D and LAROSE R (2004) Keeping our network safe: a model of online safety behavior. *Proceedings of the Association for Education in Journalism and Mass Communication*, Toronto, Canada.

LENT RW, HOFFMAN MA, HILL CE, TREISTMAN D, MOUNT M and SINGLEY D (2006) Client-specific counselor self-efficacy in novice counselors: relation to perceptions of session quality. *Journal of Counseling Psychology* **53,** 453–463.

MALHOTRA NK, KIM SS and PATIL A (2006) Common method variance in IS research: a comparison of alternative approaches and a reanalysis of past research. *Management Science* **52(12),** 1865–1883.

MARAKAS GM, JOHNSON RD and CLAY PF (2007) The evolving nature of the computer self-efficacy construct: an empirical investigation of measurement construction, validity, reliability, and stability over time. *Journal of the Association for Information Systems* **8(1),** 16–46.

MCCLENDON BT and PRENTICE-DUNN S (2001) Reducing skin cancer risk: an intervention based on protection motivation theory. *Journal of Health Psychology* **6,** 321–328.

MCMATH BF and PRENTICE-DUNN S (2005) Protection motivation theory and skin cancer risk: the role of individual differences in responses to persuasive appeals. *Journal of Applied Social Psychology* **35,** 621–635.

MILNE S, SHEERAN P and ORBELL S (2000) Prediction and intervention in health-related behavior: a meta-analytic of protection motivation theory. *Journal of Applied Social Psychology* **30(1),** 106–143.

ORLIKOWSKI WJ (1992) The duality of technology: rethinking the concept of technology in organizations. *Organization Science* **3(3),** 398–427.

PECHMANN C, ZHAO G, GOLDBERG ME and REIBLING ET (2003) What to convey in antismoking advertisements for adolescents: the use of protection motivation theory to identify effective message theme. *Journal of Marketing* **67(April),** 1–18.

PETTER S, STRAUB DW and RAJ A (2007) Specifying formative constructs in IS research. *MIS Quarterly* **31(4),** 623–656.

RIEMENSCHNEIDER CK, HARRISON DA and MYKYTYN PP (2003) Understanding IT adoption decisions in small business: integrating current theories. *Information and Management* **40(4),** 269–285.

ROGERS R (1983) Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In *Social Psychophysiology: A Sourcebook* (Cacioppo J and Petty R, Eds), pp 153–176, Guilford Press, New York.

STRAUB DW (1989) Validating instruments in MIS research. *MIS Quarterly* **13(2),** 147–169.

STRAUB DW, WEILL P and SCHWAIG KS (2008) Strategic dependence on the IT resource and outsourcing: a test of the strategic control model. *Information Systems Frontier* **10,** 195–210.

STRAUB DW and WELKE RJ (1998) Coping with systems risk: security planning models for management decision making. *MIS Quarterly* **22(4),** 441–465.

THONG JYL (1999) An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems* **15(4),** 187–214.

VENKATESH V, MORRIS MG, DAVIS GB and DAVIS FD (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly* **27(3),** 425–478.

WILLISON R and BACKHOUSE J (2006) Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems* **15(4),** 403–414.

WOLD H (1982) Soft modelling: the basic design and some extensions. In *Systems Under Indirect Observation, Part II* (Jöreskog, K. and Wold W. Eds), North Holland Press, Amsterdam.

WOON IMY, TAN GW and LOW RT (2005) A protection motivation theory approach to home wireless security. In *Proceedings of the Twenty-Sixth International Conference on Information Systems* (AVISON D, GALLETTA D and DEGROSS J, Eds), Las Vegas, NV, pp 367–380.

ZHAO G and PECHMANN C (2007) The impact of regulatory focus on adolescents' response to antismoking advertising campaigns. *Journal of Marketing Research* **XLIV,** 671–687.

Appendix

See Table A1.

Table A1 Instrument items

Construct	*Mean (SD)*	*Reference*	*Instrument items*
Perceived severity	4.166 (0.816)	Woon *et al.* (2005)	How strongly do you disagree or agree with the following statements? • Malware poses a severe security risk to our networks and systems. • Malware can transmit sensitive data to third parties (e.g., passwords, usernames, customer information). • Malware can allow remote access to our computers. • Malware can be used to download and install malicious applications.
Perceived vulnerability	3.675 (0.929)	Pechmann *et al.* (2003)	How likely is malware to affect your computers in the following ways? • Transmit sensitive data to third parties. • Allow access to remote attackers. • Install malicious applications.
Response efficacy	3.909 (0.761)	Pechmann *et al.* (2003)	Installing antimalware software will successfully prevent malware attacks. Antimalware software is the best solution for counteracting problems caused by malware. If we install antimalware software on our computers, we can minimize the threat of malware.
Self-efficacy	3.893 (0.786)	Lent *et al.* (2006)	It is easy for us to install and manage antimalware software on our computers. We can perform system updates on antimalware software by ourselves. We have the capability to solve possible system errors or problems during the installation and operation of antimalware software (e.g., system crash).
Response cost	3.487 (0.957)	Venkatesh *et al.* (2003)	Antimalware software is expensive to purchase and operate. We have to upgrade our computers to install antimalware software. Antimalware software can slow down our computers.
Social influence	3.697 (0.790)	Ho (2000)	Our competitors have adopted or are in the process of adopting antimalware software. Our partner companies who share important business information with us believe we should adopt antimalware software. The customers of our company believe that we should adopt antimalware software for keeping customer-related data safe from Malware attacks.
Vendor support	3.904 (0.968)	Addis (2003)	Our vendors provide a designated technician (or groups of technicians) to help with the difficulties of using antimalware software. Our vendors offer training workshops on how to use antimalware software. Our vendors provide us with a hot-line or 24/7 technical support for problems caused by malware.
Adoption intention	4.084 (0.833)	Venkatesh *et al.* (2003)	I intend to support my company's purchases of antimalware software. It is very likely that I will encourage my company to financially support the purchases of antimalware software.
Actual adoption	1.787 (0.411)		The purchases of antimalware software (y/n).
IT budgets	4.490 (1.585)	Kambil *et al.* (2000)	IT Budget in 2006 IT Budget in 2007
Firm size	6.393 (2.095)	Forman (2005)	Number of employees Number of PCs

In this study, we separated the construct 'IT budget' from 'response cost.' IT budget is associated with total IT resources in SMBs, while response cost assesses the cost directly associated with protective systems adoption.