Ollscoil na Gaillimhe
University of Galway

Provided by the author(s) and University of Galway in accordance with publisher policies. Please cite the published version when available.

Title	Linking threat avoidance and security adoption: a theoretical model For SMEs
Author(s)	Browne, Sean; Lang, Michael; Golden, Willie
Publication Date	2015-06-07
Publication Information	Browne, Sean; Lang, Michael; and Golden, Willie, "Linking Threat Avoidance and Security Adoption: A Theoretical Model For SMEs" (2015). BLED 2015 Proceedings. 35. http://aisel.aisnet.org/bled2015/35
Publisher	AIS Electronic Library (AISeL)
Link to publisher's version	https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1002&context=bled2015
Item record	http://hdl.handle.net/10379/14595

Downloaded 2024-05-22T17:06:52Z

Some rights reserved. For more information, please see the item record link above.

28th Bled eConference

#WellBeing

June 7 - 105, 2015; Bled, Slovenia

Linking Threat Avoidance and Security Adoption: *A Theoretical Model For SMEs*

Sean Browne

National University of Ireland Galway, Ireland

s.browne2@nuigalway.ie

Michael Lang

National University of Ireland Galway, Ireland

michael.lang@nuigalway.ie

Willie Golden

National University of Ireland Galway, Ireland

willie.golden@nuigalway.ie

Abstract

A deficiency exists in the Information Systems Security literature because of the tendency to regard IT threat avoidance and IT security adoption as separate behaviours. In addressing the deficiency this research in progress focuses on SMEs, for several reasons including their strategic importance globally, the current trend among cybercriminals to conduct more high volume, low risk attacks against weaker targets and also because of the individualistic behavioural patterns in SMEs. Drawing on several well-established behavioural theories, this paper synthesises elements of these theories into a holistic model, with coping theory placed firmly at is centre. This study will make several contributions to the field, initially creating an empirically validated model for behaviours surrounding both avoidance and preventative actions in small firms and also in presenting and prioritising a specific view of the external factors influencing how threats are appraised, assessed and dealt with.

Keywords: *Cybercrime, Threat, Avoidance, Adoption, Protection Motivation, Self-Efficacy, Coping, Security.*

1 INTRODUCTION

This research in progress is motivated by a number of factors both theoretical and practical, with two overarching motivations. The first stems from the fact that computer crime is becoming both epidemic and inexorable in its evolution. The second and

equally fundamental motivation is that SMEs are becoming more and more important in the world's economies, particularly as those economies become more e-driven.

In adopting a holistic approach we argue that although adoption and avoidance are fundamentally different behaviours (Carver & White, 1994; Elliot & Covington, 2001), they are inexorably linked and need to be viewed in conjunction with each other. To deal with this we develop a theoretical model through synthesis of existing constructs that, to the best of our knowledge, uniquely examines the symbiotic nature of IT threat avoidance and IT security adoption in the SME sector.

1.1 SMEs

The term SME is generally understood to refer to companies with fewer than 250 employees and with annual turnover not exceeding €50 million (EU Commission, 2005), and are of particular interest for several reasons. Firstly, industry reports have highlighted that cybercrime is moving towards automated high-volume, low-risk attacks against weaker targets (Verizon, 2012). This exposure is amplified by the fact that threats have increased faster than potential victims - or cyber security professionals - can cope with them (Deloitte & Touche, 2010), with attacks on small businesses being on the increase (PWC, 2013) and comprising in excess of 60% of reported data breaches (PWC, 2013; Verizon, 2012).

Secondly, an equally compelling reason for focussing on SMEs is the fact that the sector, is a significant and critical stratum in most major economies, comprising the vast majority of firms in North America (USITC, 2010) and Europe, the latter having 90% of companies that are micro firms of 10 employees or less (ECORYS, 2012). Additionally small entrepreneurial firms are emerging as the sector with the highest cloud adoption rate (Subashini & Kavitha, 2011). This fact, coupled with the assessment of the cloud by some commentators indicating a recurrence of the same mistakes that were made with initial Internet development of precedence being given to functionality and performance at the expense of security (Chonka, Xiang, Zhou, & Bonti, 2011), is a real concern for SMEs.

The justification for the development of a separate behavioural model comes from a belief that small companies "think" and behave differently in computer security matters to larger firms. In small firms, the work environment is invariably busy and hectic (Baron, 2000, 2004) and often characterised by "brevity and high levels of fragmentation" (Mueller, Volery, & von Siemens, 2012), with decision making typified by a heuristic-based management style (Dewald & Bowen, 2010; Westhead, Ucbasaran, & Wright, 2005). This sometimes results in non-value added activities - like IS security - being relegated in the pecking order.

In essence, our contention is that there are enough differences in SME behaviour to justify the preparation of a separate behavioural model, and our challenge is to integrate our knowledge of general management behaviour into the information systems security knowledge base.

1.2 Behaviour

It is well accepted that in today's e-world, security solutions extend beyond technology and involve organisational, environmental and behavioural factors (Herath & Rao, 2009) requiring an understanding of the weakest link in the defence against security threats: human behaviour and attitudes (Dinev & Hu, 2007).

The enterprise and small business management literature, in particular is rife with the notion of a dominant leader (Dewald & Bowen, 2010; Misra & Kumar, 2000; Westhead et al., 2005) using a mixture of thinking styles. This suggests there is a certain legitimacy to anthropomorphising organisational behaviours (Bhattacherjee, 2002), an approach we have adopted in our model.

2 LITERATURE REVIEW AND HYPOTHESES

The essential contribution of this paper lies in creating a theoretical model, which examines the interrelated nature of IT threat avoidance and IT security adoption behaviours, and the following subsections deal with the individual elements of that model.

2.1 AVOIDANCE

Avoidance in the context of information security is not just a reflexive or affective act, but rather comprises a number of stages of appraisal and coping with a particular threatening situation in order to affect some level of self-preservation. In order to understand this notion we begin with a review of Protection Motivation Theory (PMT).

Protection Motivation Theory

The theory postulates that when an individual is exposed to persuasive communications about undesirable consequences of a particular event, that these communications initiate a series of cognitive appraisal processes resulting in attitude change (Rogers, 1975).

In a subsequent revision of the theory, Rippetoe and Rogers (1987) describe a secondary process called coping appraisal. In this process, the efficacy component is moderated by what are described as Response Costs, which include the time, effort, stress and any other reasons, which would suggest not pursuing change.

Overall the model suggests that threat appraisal is concerned with evaluating the status quo, with the likelihood of an adaptive response or a change in behaviour being increased when perceptions of severity or likelihood are high, or reduced when any rewards associated with continuing the maladaptive response are perceived (McMath & Prentice-Dunn, 2005).

Technology Threat Avoidance Theory

While the origins of PMT are in health psychology, it might seem more pertinent at this juncture to refer to the more modern Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009, 2010). TTAT subsumes PMT and it incorporates threat appraisal and coping appraisal as its main variables. In line with TTAT and the other studies underpinned by PMT, we have developed the following hypotheses by taking the variables already established in the information security literature and applying them in the context of SMEs for reasons already alluded to:

H 1: *Perceived severity of IT threats positively affects avoidance motivation in SMEs*

H 2: *Perceived likelihood of IT threats positively affects avoidance motivation in SMEs*

H 4(a): *Response efficacy in SMEs positively affects avoidance motivation*

H 4(b): *Response efficacy in SMEs negatively affects emotion-focused coping*

H 5(a): *Response costs in SMEs negatively affect avoidance motivation*

H 5(b): *Response costs in SMEs positively affect emotion-focused coping*

The real extension to PMT is derived when addressing the coping action itself. Coping theory suggests that, "when stressful conditions are viewed by a person as refractory to change, emotion focused coping predominates; when they are appraised as controllable by action, problem focused coping predominates" (Lazarus, 1993). We have included this extension to PMT in our model, to examine the phenomenon of inaction during conditions of information systems threat. This may occur as a consequence of ambivalence, ignorance or complacency and often results in companies failing to implement even the most basic of controls (Willison & Backhouse, 2006). While this notion may seem counter-intuitive, the fact remains that it does actually happen.

Risk Tolerance

Once considered a concept from the finance field, there is evidence to suggest that the concept is related to settings and demographic factors (Barsky, Juster, Kimball, & Shapiro, 1997; Faff, Hallahan, & McKenzie, 2009), and we have redefined it for the purposes of this study as "Risk Tolerance by Management in SMEs".

We have done so, because literature would suggest that organisational risk tolerance is strongly related to the origins, size and maturity of a business (Baron, 2000; Groves, Vance, & Choi, 2011; Knorr, Alvarez, & Urbano, 2013), which is a possible indication that SME's risk tolerance may be unique. In general, while risk tolerance forms part of the threat appraisal process it also affects how people respond to that threat appraisal and consequently a person or small company with low levels of risk tolerance will not be happy to tolerate a situation of perceived threat. Thus we propose:

H 3(a): *SME Risk Tolerance negatively affects avoidance motivation*

H 3(b): *SME Risk Tolerance positively affects emotion-focused coping*

Social Influence

Social influence is likely to be an important variable in any behavioural model. It has been variously described as one of the most pervasive determinants of a person's behaviour (Burnkrant & Cousineau, 1975), and pressure to accept information supplied by others as evidence of reality (Deutsch & Gerard, 1955). Because most, if not all, SMEs are part of a bigger ecosystem, Kelman's (2006) view that the process involves three processes or levels: compliance, internalisation and identification adds to the notion that far from being an opaque idea, social influence is both real and relevant. Having previously found favour in the information systems literature (Pavlou & Fygenson, 2006; Taylor & Todd, 1995; Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & Davis, 2003), social influence can be said to significantly colour behaviour. Thus we find it appropriate in the present context to suggest that SMEs do not "think" about security in a vacuum and that:

H6: *Social influence in SMEs affects emotion focused coping and avoidance motivation*

While appraisal and coping are significant cognitive processes, they do not, in themselves, represent an endgame. Considering the adjustments to behaviour illustrated by control theory (Carver & Scheier, 1982), we need to consider the cognitive processes involved in adoption behaviour, and to what extent they are the same as those underpinning the avoidance behaviour in order to reach that endgame.

2.2 ADOPTION

A rich body of literature exists surrounding the notion of acceptance and adoption behaviour, much of which is grounded in the Theory of Planned Behaviour (TPB) from the psychology literature and the Technology Acceptance Model (TAM) in the information systems field. Both of these theories have their roots in the Theory of Reasoned Action (Ajzen, 1991), contending that a person's behaviour is determined by their intention to perform the behaviour of interest (Dinev & Hu, 2007). Most of the variables within these and similar theories have previously been adapted to the information security context and are outlined in the table below.

Table 1: Summary of relationships previously established in the literature
adapted from (Dinev & Hu, 2007)

Perceived Behavioural Control ⇢ Security Adoption Intention	(Ajzen, 1991, 2002; Mathieson, 1991; Pavlou & Fygenson, 2006; Taylor & Todd, 1995)
Subjective Norm ⇢ Security Adoption Intention	(Ajzen, 1991, 2002; Pavlou & Fygenson, 2006; Taylor & Todd, 1995; Venkatesh & Davis, 2000)
Attitude ⇢ Security Adoption Intention	(Ajzen, 1991, 2002; Davis, Bagozzi, & Warshaw, 1989; Taylor & Todd, 1995)
Perceived Ease of Use ⇢ Security Adoption Intention	(Davis et al., 1989; Gefen, Karahanna, & Straub, 2003; Gefen & Straub, 1997; Koufaris, 2002; van der Heijden, 2004; Venkatesh, 1999, 2000; Venkatesh & Davis, 1996, 2000; Venkatesh et al., 2003)
Perceived Usefulness ⇢ Security Adoption Intention	
Perceived Usefulness ⇢ Attitude	(Davis et al., 1989; Pavlou & Fygenson, 2006; Taylor & Todd, 1995)
Perceived Usefulness ⇢ Subjective Norm	(Venkatesh & Davis, 2000)
Perceived Ease of Use ⇢ Attitude	(Davis et al., 1989; Pavlou & Fygenson, 2006; Taylor & Todd, 1995)
Perceived Ease of Use ⇢ Perceived Behavioural Control	(Pavlou & Fygenson, 2006)
Self Efficacy⇢Perceived Behavioural Control	(Ajzen, 2002; Pavlou & Fygenson, 2006; Taylor & Todd, 1995)
Controllability⇢Perceived Behavioural Control	(Ajzen, 2002; Pavlou & Fygenson, 2006; Taylor & Todd, 1995)
Avoidance Motivation ⇢ Security Adoption	(Ajzen, 1991; Banerjee, Cronan, & Jones, 1998)

While several of these are relevant to security adoption behaviour we do not consider them peculiar to SMEs and consequently are not proposed for retesting as part of this study.

However, in line with our earlier argument in favour of the anthropomorphic nature of SMEs we believe it is particularly relevant to test the relationship between motivation, intention and behaviour. For example, Liang and Xue (2010) in their study of personal computer usage argue that intention is a strong predictor of actual behaviour. This view of intention as an antecedent of actual behaviour (Ajzen, 1991; Banerjee et al., 1998; Warkentin, Johnston, & Shropshire, 2011) is to be found in both the psychology and information systems literature and leads us to conclude that motivation to avoid IT threats will result in the introduction of security safeguards.

H7: *Avoidance motivation is a positive determinant of security adoption*

Self Efficacy

As a unique but subtle distinguishing feature we treat self-efficacy as the lynchpin in the integration of avoidance and adoption behaviours. This is because of our contention that in a holistic behavioural model, self-efficacy has a causal effect on both the coping disposition and actioning the decision on security adoption.

Owing much to the work of Bandura (1977), it is important to note that the concept is not exclusive to personal behaviour but is also highly relevant in the organisational context. For example, resiliency in self-efficacy has been shown to be essential for effective functioning in organisations (Bandura & Wood, 1989) where accomplishments are rarely achieved through quick successes.

Furthermore, the causal effect that self-efficacy has on coping dispositions and actions, permeates the literature extensively (Bandura & Cervone, 1983; Lazarus, 1993; Rogers, 1975), and consequently causes us to posit the following hypotheses:

H8(a): *Self-Efficacy in SMEs positively affects avoidance motivation*

H8(b): *Self-Efficacy in SMEs negatively affects emotion-focused coping*

However, self-efficacy not only has an effect on coping and motivation but also has a direct effect on actual behaviour, which is consistent with the awareness centric model of user behaviour toward protective technologies as proposed by Dinev & Hu (2007), and is also seen in the work of Taylor & Todd (1995) and Pavlou & Fygenson (2006). Therefore we also propose that:

H9: *Self-Efficacy in SMEs positively affects security adoption*

Awareness of available security options

The final major variable in our model is adapted from the concept of technology awareness (Dinev, Goo, Hu, & Nam, 2009; Dinev & Hu, 2007) and re-defined here as "a person's raised consciousness of, and interest in, knowing about security issues and strategies to deal with them". The absence of this awareness is suggested in industry reports (Verizon, 2012), and represents an obvious cause for concern. The relevance to SMEs is further emphasised by the fact that it is seen as a variable that is dependent on culture, and because SMEs represent a very particular type of organisation having their own culture, we believe that awareness of available security options is not only important in the security adoption process but also vital.

Therefore we propose that:

H10: *Awareness of available security options is a positive determinant of security adoption.*

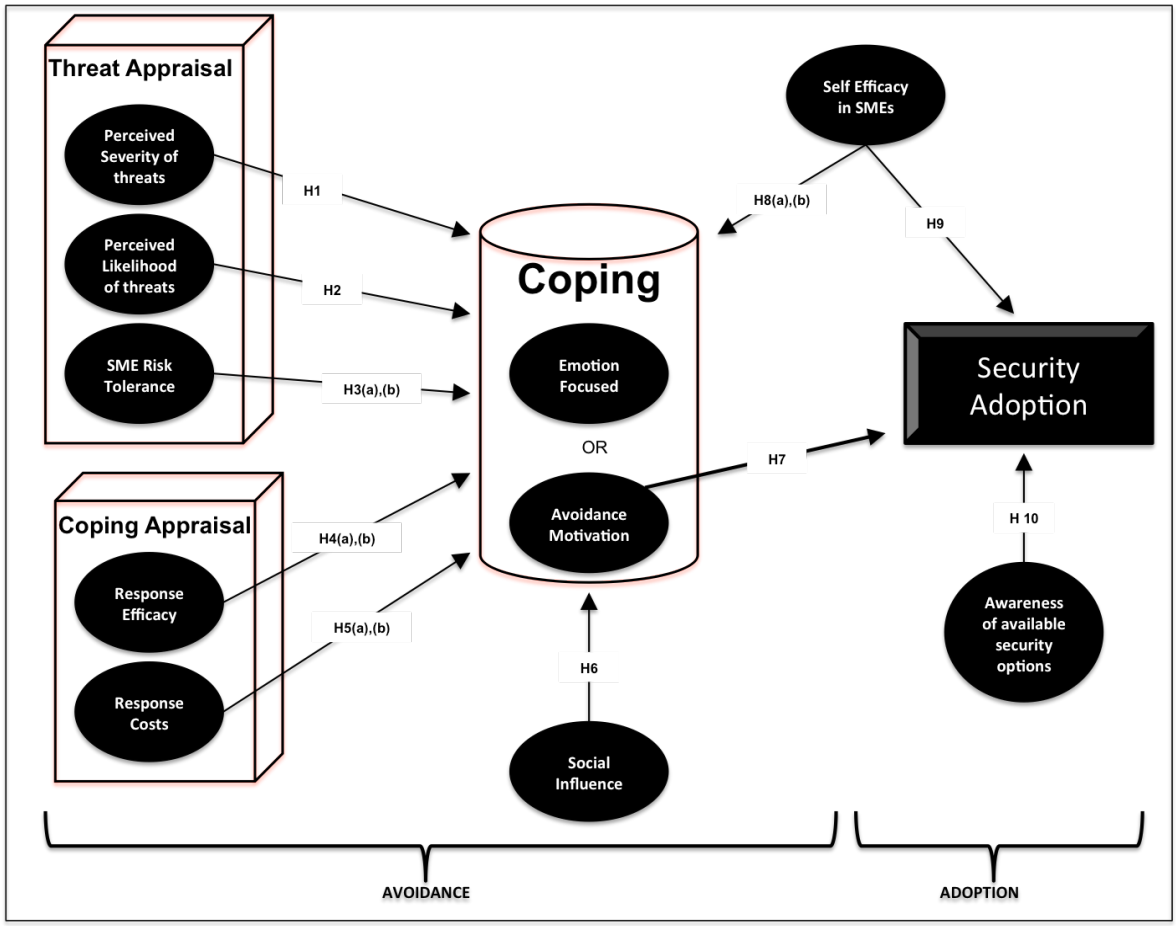

Figure 1: Proposed Research Model

3 CONCLUSION AND FURTHER WORK

In this paper we develop a theoretical model, which synthesises a multitude of theories from various strands of literature, examining both the factors that affect attitudes and behaviours of small-firm principals in dealing with malicious computer threats, and their inherent processes.

If the hypotheses are supported this model will make two contributions to practice. Firstly it will serve to predict how principals in SMEs will behave in terms of assessing security concerns and implementing responses and secondly, it will highlight priorities to be targeted in improving security in small firms.

The research will be conducted using a mixed-methods approach, a paradigm that continues to grow and gain legitimacy (Fry, Chantavanich, & Chantavanich, 1981; Johnson, Onwuegbuzie, & Turner, 2007; Morgan, 2007). In order to develop the statistical model, the empirical segment of this research will have as its foundation a

number of semi-structured interviews incorporating a series of relevant vignettes. This use of vignettes has been successfully employed in previous studies (Gattiker & Kelley, 1999; Siponen & Vance, 2010) where respondents are reluctant to answer questions that reflect badly on themselves.

Subsequently and building directly on the earlier phase the second part of this study will take the form of a large-scale industry survey, and will allow for the comparison of results with similar studies undertaken in different countries.

REFERENCES

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi: 10.1016/0749-5978(91)90020-t

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology, 32*(4), 665-683. doi: 10.1111/j.1559-1816.2002.tb00236.x

Bandura, A. (1977). Self-Efficacy - toward a Unifying Theory of Behavioral Change. *Psychological Review, 84*(2), 191-215. doi: 10.1037//0033-295x.84.2.191

Bandura, A., & Cervone, D. (1983). Self-Evaluative and Self-Efficacy Mechanisms Governing the Motivational Effects of Goal Systems. *Journal of Personality and Social Psychology, 45*(5), 1017-1028. doi: 10.1037//0022-3514.45.5.1017

Bandura, A., & Wood, R. (1989). Effect of Perceived Controllability and Performance Standards on Self-Regulation of Complex Decision-Making. *Journal of Personality and Social Psychology, 56*(5), 805-814. doi: 10.1037//0022-3514.56.5.805

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT Ethics: A Study in Situational Ethics. *MIS Quarterly, 22*(1), 31-60. doi: 10.2307/249677

Baron, R. A. (2000). Counterfactual Thinking and Venture Formation: The Potential Effects of Thinking About "What Might Have Been". *Journal of Business Venturing, 15*(1), 79-91. doi: 10.1016/s0883-9026(98)00024-x

Baron, R. A. (2004). Potential Benefits of the Cognitive Perspective: Expanding Entrepreneurship's Array of Conceptual Tools. *Journal of Business Venturing, 19*(2), 169-172. doi: 10.1016/s0883-9026(03)00004-1

Barsky, R. B., Juster, F. T., Kimball, M. S., & Shapiro, M. D. (1997). Preference Parameters and Behavioral Heterogeneity: An Experimental Approach in the Health and Retirement Study. *Quarterly Journal of Economics, 112*(2), 537-579. doi: 10.1162/003355397555280

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems, 19*(1), 211-241.

Burnkrant, R. E., & Cousineau, A. (1975). Informational and Normative Social Influence in Buyer Behavior. *Journal of Consumer Research, 2*(3), 206-215. doi: 10.1086/208633

Carver, C. S., & Scheier, M. F. (1982). Control-Theory - a Useful Conceptual-Framework for Personality-Social, Clinical, and Health Psychology. *Psychological Bulletin, 92*(1), 111-135. doi: 10.1037//0033-2909.92.1.111

Carver, C. S., & White, T. L. (1994). Behavioral-Inhibition, Behavioral Activation, and Affective Responses to Impending Reward and Punishment - the BIS BAS Scales. *Journal of Personality and Social Psychology, 67*(2), 319-333. doi: 10.1037//0022-3514.67.2.319

Chonka, Ashley, Xiang, Yang, Zhou, Wanlei, & Bonti, Alessio. (2011). Cloud Security Defence to Protect Cloud Computing against Http-DoS and Xml-DoS Attacks. *Journal of Network and Computer Applications, 34*(4), 1097-1107. doi: 10.1016/j.jnca.2010.06.004

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer-Technology - a Comparison of 2 Theoretical-Models. *Management Science, 35*(8), 982-1003. doi: 10.1287/mnsc.35.8.982

Deloitte & Touche. (2010). Cyber Crime: A Clear and Present Danger Combating the Fastest Growing Cyber Security Threat.

Deutsch, M., & Gerard, H. B. (1955). A Study of Normative and Informational Social Influences Upon Individual Judgement. *Journal of Abnormal Psychology, 51*(3). doi: 10.1037/h0046408

Dewald, J., & Bowen, F. (2010). Storm Clouds and Silver Linings: Responding to Disruptive Innovations through Cognitive Resilience. *Entrepreneurship Theory and Practice, 34*(1), 197-218.

Dinev, Tamara, Goo, Jahyun, Hu, Qing, & Nam, Kichan. (2009). User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences. *Information Systems Journal, 19*(4), 391-412. doi: 10.1111/j.1365-2575.2007.00289.x

Dinev, Tamara, & Hu, Qing. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems, 8*(7), 386-408.

ECORYS. (2012). EU SMEs in 2012: At the Crossroads Annual Report on Small and Medium-Sized Enterprises in the EU, 2011/12. Rotterdam: European Commission.

Elliot, A. J., & Covington, M. V. (2001). Approach and Avoidance Motivation. *Educational Psychology Review, 13*(2), 73-92.

EU Commission. (2005). *The New SME Definition*: European Commission Publications Office.

Faff, R., Hallahan, T., & McKenzie, M. (2009). Nonlinear Linkages between Financial Risk Tolerance and Demographic Characteristics. *Applied Economics Letters, 16*(13), 1329-1332. doi: 10.1080/13504850701381123

Fry, G., Chantavanich, S., & Chantavanich, A. (1981). Merging Quantitative and Qualitative Research Techniques - toward a New Research Paradigm. *Anthropology & Education Quarterly, 12*(2), 145-158. doi: 10.1525/aeq.1981.12.2.05x1889q

Gattiker, U. E., & Kelley, H. (1999). Morality and Computers: Attitudes and Differences in Moral Judgments. *Information Systems Research, 10*(3), 233-254. doi: 10.1287/isre.10.3.233

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly, 27*(1), 51-90.

Gefen, D., & Straub, D. W. (1997). Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model. *MIS Quarterly, 21*(4), 389-400. doi: 10.2307/249720

Groves, K., Vance, C., & Choi, D. (2011). Examining Entrepreneurial Cognition: An Occupational Analysis of Balanced Linear and Nonlinear Thinking and Entrepreneurship Success. *Journal of Small Business Management, 49*(3), 438-466. doi: 10.1111/j.1540-627X.2011.00329.x

Herath, Tejaswini, & Rao, H. Raghav. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems, 18*(2), 106-125. doi: 10.1057/ejis.2009.6

Johnson, R. Burke, Onwuegbuzie, Anthony J., & Turner, Lisa A. (2007). Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research, 1*(2), 112-133. doi: 10.1177/1558689806298224

Kelman, H. C. (2006). Interests, Relationships, Identities: Three Central Issues for Individuals and Groups in Negotiating Their Social Environment *Annual Review of Psychology* (Vol. 57, pp. 1-26).

Knorr, H., Alvarez, C., & Urbano, D. (2013). Entrepreneurs or Employees: A Cross-Cultural Cognitive Analysis. *International Entrepreneurship and Management Journal, 9*(2), 273-294. doi: 10.1007/s11365-012-0235-2

Koufaris, M. (2002). Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behavior. *Information Systems Research, 13*(2), 205-223. doi: 10.1287/isre.13.2.205.83

Lazarus, R. S. (1993). Coping Theory and Research - Past, Present, and Future. *Psychosomatic Medicine, 55*(3), 234-247.

Liang, Huigang, & Xue, Yajiong. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*(1), 71-90.

Liang, Huigang, & Xue, Yajiong. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Mathieson, Kieran. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research, 2*(3), 173-191. doi: citeulike-article-id:5428229

McMath, B. F., & 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*(3), 621-643. doi: 10.1111/j.1559-1816.2005.tb02138.x

Misra, Sasi, & Kumar, E. Sendil. (2000). Resourcefulness: A Proximal Conceptualisation of Entrepreneurial Behaviour. *Journal of Entrepreneurship, 9*(2), 135-154. doi: 10.1177/097135570000900201

Morgan, D. L. (2007). Paradigms Lost and Pragmatism Regained Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research, 1*(1), 48-76. doi: 10.1177/2345678906292462

Mueller, S., Volery, T., & von Siemens, B. (2012). What Do Entrepreneurs Actually Do? An Observational Study of Entrepreneurs' Everyday Behavior in the Start-up and Growth Stages. *Entrepreneurship Theory and Practice, 36*(5), 995-1017. doi: 10.1111/j.1540-6520.2012.00538.x

Pavlou, P. A., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly, 30*(1), 115-143.

PWC. (2013). *2013 Information Security Breaches Survey*. United Kingdom: Department for Business Information & Skills.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat. *Journal of Personality and Social Psychology, 52*(3), 596-604. doi: 10.1037//0022-3514.52.3.596

Rogers, R. W. (1975). Protection Motivation Theory of Fear Appeals and Attitude-Change. *Journal of Psychology, 91*(1), 93-114.

Siponen, Mikko, & Vance, Anthony. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-502.

Subashini, S., & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications, 34*(1), 1-11. doi: 10.1016/j.jnca.2010.07.006

Taylor, S., & Todd, P. A. (1995). Understanding Information Technology Usage - a Test of Competing Models. *Information Systems Research, 6*(2), 144-176. doi: 10.1287/isre.6.2.144

USITC. (2010). Small and Medium- Sized Enterprises: Overview of Participation in U.S. Exports: United States International Trade Commission;.

van der Heijden, H. (2004). User Acceptance of Hedonic Information Systems. *MIS Quarterly, 28*(4), 695-704.

Venkatesh, V. (1999). Creation of Favorable User Perceptions: Exploring the Role of Intrinsic Motivation. *MIS Quarterly, 23*(2), 239-260. doi: 10.2307/249753

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information Systems Research, 11*(4), 342-365. doi: 10.1287/isre.11.4.342.11872

Venkatesh, V., & Davis, F. D. (1996). A Model of the Antecedents of Perceived Ease of Use: Development and Test. *Decision Sciences, 27*(3), 451-481. doi: 10.1111/j.1540-5915.1996.tb00860.x

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, 46*(2), 186-204. doi: 10.1287/mnsc.46.2.186.11926

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

Verizon. (2012). 2012 Data Breach Investigations Report.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention. *European Journal of Information Systems, 20*(3), 267-284. doi: 10.1057/ejis.2010.72

Westhead, P., Ucbasaran, D., & Wright, M. (2005). Experience and Cognition - Do Novice, Serial and Portfolio Entrepreneurs Differ? *International Small Business Journal, 23*(1), 72-98. doi: 10.1177/0266242605049104

Willison, Robert, & Backhouse, James. (2006). Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective. *European Journal of Information Systems, 15*(4), 403-414. doi: 10.1057/palgrave.ejis.3000592