Cloud Security Consciousness: A Need for Realisation in Entrepreneurial Small Firms

Sean Browne
s.browne2@nuigalway.ie

Michael Lang
michael.lang@nuigalway.ie

Business Information Systems, National University of Ireland Galway

Abstract

Cloud computing represents a fundamental shift in the way information services are provided but with its unique architecture comes additional security challenges, many of which are technical in nature. However, the paradigm shift also presents new challenges, which are non-technical and whether or not companies actually consider all of these issues in moving to the cloud is a matter of concern.
This paper attempts to elevate the notion of cloud security consciousness (CSC) in the domain of small firms with a goal of introducing a level of innateness into the concept in its practical use.
By synthesising CSC with various behavioural theories including coping theory, we seek to place CSC and the coping process at the centre of a security-centric cognitive framework for cloud adoption, while recognising that such coping processes are heavily shaped by both social influence and self-efficacy factors.

Keywords: Cloud computing, Security, Threats, Coping, Behaviour

1.0 Introduction

The terms ‘nascent’, ‘emerging’ and ‘disruptive’ are extensively used throughout the extant literature to describe the cloud-computing paradigm, even extending to the literature in the cloud security sphere (Marston et al., 2011, Sehgal et al., 2011, Kshetri, 2013). Whether these are appropriate terms and the paradigm is actually new or not is a moot point, with suggestions coming from some quarters that a more appropriate view is to consider it as a natural evolution of technology, economy and culture (Takabi et al., 2010). However, what is not in dispute is that cloud computing’s pervasiveness represents a disruptive change in how information technology is supplied. In recognising that reality, this paper synthesises aspects of the cloud security literature with behavioural theories, particularly those situated in the entrepreneurship literature pertaining to small firms. In a unique contribution to the field we recommend a conceptual framework that places coping at the centre of the adoption decision process in small entrepreneurial firms.

As with all evolutionary phenomena, what is most important is that we learn from the past, a point that is oft repeated in the information systems literature because in practice it often emerges that “issues seen as ‘new’ turn out to have long roots” (Keen, 1991). In the case of cloud computing, some commentators suggest that we are experiencing a recurrence of the same mistakes that were made with initial internet development, where precedence was given to functionality and performance at the expense of security (Chonka et al., 2011). It is acknowledged that because of its deployment method, the cloud is fraught with security risks - effectively taking on vulnerabilities of existing web applications (Subashini and Kavitha, 2011). Of significance too is the view that the paradigm “amplifies computer security issues” (Sehgal et al., 2011) coupled with the contention that these issues will only be exacerbated as more data is saved and backed up to the cloud (Hyman, 2013). These concerns are further complicated by the fact that threats can come from both inside and outside the cloud, resulting in security concerns being cited as the most significant barrier to cloud adoption (Armbrust et al., 2010, Kshetri, 2013, Xiao and Xiao, 2013).

Therefore it now seems appropriate to develop an adoption model that places security at the centre of the model rather than on the periphery. The motivation to focus on small firms in this study arises for several reasons. Firstly, the small-to-medium (SME) sector is now being recognised as a significant and critical stratum in most major economies,

comprising the vast majority of firms in North America (USITC, 2010) with an equally pronounced importance in Europe, where it contributes more than half of the total value-added by business and provides two thirds of private sector jobs. This polarisation in economic demographics is further illustrated by the fact that 90% of these private sector jobs are in micro firms of 10 employees or less (ECORYS, 2012). The second, but equally important, reason for focussing on small firms is that small entrepreneurial firms are emerging as the sector with the highest cloud adoption rate (Subashini and Kavitha, 2011).

While economic significance and adoption policy trends may pique our interest in the SME sector, justification for the establishment of a separate behavioural model comes from a belief that small companies think and behave differently in computer security matters than larger firms. An example is the finding that for many SMEs, their failure to plan the introduction and exploitation of new technology is due to management limitations, with the age and experience of the owner being frequently cited as the most important factor (Levy et al., 2001). Relying heavily on a heuristic-based management style (Westhead et al., 2005, Dewald and Bowen, 2010, Endres and Woods, 2006), many small firms' principals appear too busy to devote time and cognitive effort to routine tasks. This phenomenon may explain observations in the literature that one of cloud computing's perceived benefits is to simply deflect cybersecurity concerns (Kaufman, 2009) or to simplify security issues by outsourcing them to someone who is highly skilled in that department (Anthes, 2010).

We therefore suggest that the time is ripe to formally introduce the concept of cloud security consciousness (CSC), which we define as:

> *An active awareness of the elements of the cloud-computing paradigm that give rise to issues of confidentiality, integrity, availability, accountability and auditability of information and information processing and an alertness to events that impact on these issues.*

Through synthesising CSC with a variant of Technology Threat Avoidance Theory (Liang and Xue, 2009, 2010) and Coping Theory, we present a holistic security-centric framework for small companies to use in proceeding with cloud adoption. With its central tenet being the coping process the framework also acknowledges the effect that self-efficacy and social influence can have on organisational coping processes.

2.0 Adoption Framework

This development of the theoretical framework is contained in the following sub-sections and is organised as follows: The next sub-section plots the landscape on security issues from the literature that arise directly as a result of the architecture of the cloud. The following sub-section introduces the concept of cloud security consciousness and its constituent elements with the following two sections discussing the impacts on organisational cognitions and coping processes, respectively.

2.1 Cloud Architecture

Many concerns about security in the cloud relate to its architecture. While the architecture continues to evolve, one of the most cited and accepted descriptions of the model remains the definition by Mell & Grance (2011) comprising 5 essential characteristics, 3 service models – Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and 4 deployment models – Private, Public, Community and Hybrid Clouds. A simple multiplication of the 5 characteristics x 3 service models x 4 deployment levels, yields a total of 60 separate domains in which security issues can present themselves (Baars and Spruit, 2012) and as new deployment models continue to emerge, such as virtual private clouds, this number of domains increases exponentially.

Focusing on the service models indicates the extent of the complication in security concerns, relating to the inherent trade-off between extensibility and security that pertains in the different models. Generally SaaS provides the least extensibility but with the provider bearing a high level of responsibility for security, while IaaS provides most extensibility but very little security capabilities and functionality (the exception being the security of the infrastructure itself), with PaaS somewhere in the middle. Furthermore, the concept of vertical heterogeneity, whereby a consumer may have differing IaaS, PaaS and SaaS providers, introduces concerns because providers' security assumptions may not be congruent when aggregated (Takabi et al., 2010).

Deployment models and methods also offer up security concerns, which may at times seem idiosyncratic. One of the points often raised about cloud computing is that the "inside the firewall and outside the firewall" paradigm doesn't work (Peterson, 2010, Kaufman, 2010). While this is true of public, community and hybrid deployments, it is not necessarily true of private clouds and as such represents a further architecture-related security concern if the private cloud security model is erroneously assumed to

exist in the other types of cloud. The technologies delivering the infrastructure also present security issues. Cloud services, in order to make sense financially and technologically, are generally enabled by virtualisation technologies in a multi-tenant model (CSA, 2009). What this means in practice is that users from disparate backgrounds like financial institutions, educators, or cybercriminals could be sharing computing resources (Kaufman, 2009). Such co-resident placement of an adversary's virtual machine has been demonstrated to be achievable in practice (Ristenpart et al., 2009), made all the more notable because the provider was the world's leading cloud infrastructure provider.

2.2 Cloud Security Consciousness (CSC)

However, it is not just the architecture of the cloud itself that presents a cause for concern. So too does the way in which we think about the cloud. Such thoughts can be anomalous with the cloud's virtuous features of flexibility and rapid provisioning also being viewed as serious security obstacles (Chen et al., 2012) or even as a security nightmare (Talbot, 2010). The added tendency to view information security as simply a synonym for hacking protection, when in fact it is much more, creates further motivation to develop the concept of Cloud Security Consciousness (CSC).

While use of the word consciousness connotes a certain sentience or perception of issues or events, the reality of the inherent cognitive limitations of human beings implies that even when we are conscious of a phenomenon we cannot be aware of every detail of that phenomenon. Therefore, to have a realistic or workable framework for consciousness, we need some categorisation or grouping system of manageable blocks or frames of reference.

Some examples include those put forward by Subashini and Kavitha (2011) who suggest that security issues can be addressed from four fronts; security related to third party resources, application security, data transmission security and data storage security. Similarly the European Union Agency for Network and Information Security identified 35 types of risk and classified them into three categories; policy and organisational, technical and legal (ENISA, 2009), while the Cloud Security Alliance has identified 13 categories of security risk and grouped them under the headings of cloud architecture, governing in the cloud and operating in the cloud.

However a more ubiquitous classification adapted, and extended, for our framework is that proposed by Kaufman (2009), who argues that a security model must promote ***confidentiality, integrity*** and ***availability*** (CIA).

Confidentiality has a particular resonance in the cloud context because of the additional possibility of cross virtual machine attack via side channels (Modi et al., 2013) and breaches by cloud administration personnel. These are regularly discussed in academic literature along with appropriate defence strategies, but whether they are considered in practice is moot. It has been suggested that privacy-preservability should also be added as an attribute (Xiao and Xiao, 2013), but the fact that this can be viewed as extreme confidentiality renders it more a measure of degree rather than a separate attribute, an approach that we have taken in our framework.

Integrity threats can come from cloud providers either maliciously or accidentally losing data or not doing appropriate computation and the latter in particular can subsequently be difficult to detect due to the lack of transparency in the relationship between parties (Xiao and Xiao, 2013).

These two issues of confidentiality and integrity are the subject of much discussion in the literature with various solutions or responses being suggested which range from encryption-based solutions to using a Trusted Third Party (Zissis and Lekkas, 2012, Vaquero et al., 2011) or Third Party Auditor (Wang et al., 2011, Xiao and Xiao, 2013). However, existence in literature does not imply consciousness in practice and while confidentiality and integrity are the two most common elements of security consciousness, they do not represent the complete picture.

Availability vulnerabilities are of particular concern with cloud service provision and can arise for a number of reasons including flooding attacks that cause a denial of service (DOS) or Fraudulent Resource Consumption (FRC) attacks (Xiao and Xiao, 2013). A further vulnerability can result from an infrastructure failure or the economic failure of the providers (Baars and Spruit, 2012, Xiao and Xiao, 2013, Modi et al., 2013). Interestingly an ENISA survey of the European public sector found that while availability is a well-defined security parameter in Security Level Agreements (SLAs), other security parameters are less well covered (ENISA, 2011).

More recently it has been suggested that the CIA triad does not adequately cover the complexities of cloud computing and that attributes of ***accountability*** and ***auditability*** need to be added (Baars and Spruit, 2012). This extension has been incorporated in our model of consciousness.

Accountability threats are primarily based around violations of SLAs or inaccurate billing of resource consumption. While some may perceive SLAs as ensuring ultimate security, there is an implicit criticism in the call for the development of SLAs using a

more bilateral approach (Rebollo et al., 2012). The purpose of such an approach is to balance the bias of the agreements, which currently tend to favour the provider's priorities, and to address peculiarities that can only be addressed at local or regional levels. This issue of accountability is articulated by Sood (2012) when he suggests that "cloud service providers cannot be trusted blindly".

Auditability is a somewhat less obvious attribute in a model of consciousness. It is implied as a means of ensuring confidentiality but also has a more explicit existence regarding regulatory requirements such as contained in the Sarbanes-Oxley legislation, Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) and Data Protection regulations. With corporate data, auditability is of critical importance (Armbrust et al., 2010) and, in the cloud context in particular, has different implications for different business locations.

This awareness of ***confidentiality, integrity***, ***availability***, ***accountability*** and ***auditability,*** or lack thereof, and the need to escalate them to a level of innateness is succinctly highlighted by security expert Bruce Schneir in (Hyman, 2013), when he comments: "Facebook has your data because you gave it to them".

Because decisions are made by humans and information security is seen as a socio-technological problem requiring an in depth understanding of human behaviour and attitudes (Dinev and Hu, 2007), we posit that cloud security consciousness (CSC) should exist at the beginning of the cloud adoption process, leading us to the following proposition:

> *P1: Cloud security consciousness comprised of confidentiality, integrity, availability, accountability and auditability should exist at the beginning of an effective cloud adoption decision process.*

2.3 Organisational Cognitions

Following on from the concept of consciousness is the notion of cognition. The former concept remains relatively inert without examining the use to which it is put, and the latter, which can be defined as "all processes by which the sensory input is transformed, reduced, elaborated, stored, recovered, and used"(Neisser, 1967), transforms the consciousness into a form usable by decision makers.

In general, cognition and cognitive psychology involve the study of individual perceptions, memory and thinking (Mitchell et al., 2002), but the issue for this paper is the appropriateness of applying cognition based theories, originally designed around individual behaviour, to small firm behaviour.

In general, the thinking of groups of individuals is different to the aggregation of their individual thoughts, and is often represented by congregate or shared mental models (Shepherd and Krueger, 2002, West, 2007). Small entrepreneurial firms, seem to exhibit somewhat different behaviours with a recurring theme in this area of literature being the notion of a dominant leader (Misra and Kumar, 2000, Westhead et al., 2005, Dewald and Bowen, 2010). In fact, what the literature seems to suggest, is a type of thinking and behaviour in entrepreneurial small firms, characterised by dominant personalities who use a mixture of cognitive and emotional thinking styles. Therefore, to consider anthropomorphising small firms (Bhattacherjee, 2002) seems appropriate and leads to the conclusion that to fully examine the behaviour of small companies protective actions regarding cloud security consciousness (CSC) requires an understanding of individuals' general threat avoidance behaviour (Liang and Xue, 2009).

In pursuit of this understanding in the context of IS security concerns, we begin with a review of Protection Motivation Theory (PMT) which has heretofore gained considerable traction in the IS literature. PMT (Rogers, 1975), as initially developed, suggested three crucial components of a fear appeal: (a) the magnitude of noxiousness of a depicted event; (b) the probability of that event's occurrence; and (c) the efficacy of a protective response. In the context of cloud adoption we suggest that the fear appeal is actually the level of CSC discussed above. The theory (PMT) postulates that protection motivation occurs from the cognitive appraisal of these three components along with the belief that a recommended coping response (in this case cloud adoption) can effectively prevent the occurrence of aversive event(s) (Rogers, 1975).

While PMT goes some way towards explaining an individual's self-preservation behaviour, its origins are in health psychology and, on its own, it does not specifically address behaviours in the context of IS. Thus, we defer to Technology Threat Avoidance Theory (TTAT) (Liang and Xue, 2009, 2010). TTAT subsumes Protection Motivation Theory (PMT) and in incorporating threat appraisal and coping appraisal as its main variables, suggests that a firm will assess the security concerns it receives from CSC and cognitively appraise them in terms of their severity of business impact, likelihood of occurrence and avoidability of occurrence. In a corroborating finding, Kshetri (2013) suggests that a company's cloud adoption decision may depend on its perception of the provider's ability to protect data from third parties and to make the data available when needed, combined with a trust in the 'bone fides' of the provider.

Our contention is that the suggestion offered by Kshetri and others is a necessary but not sufficient rationale for cloud adoption, and thus our second proposition becomes:

P2: Small firms evaluate the contents of their security consciousness against the criteria of perceived severity, likelihood and avoidability, which affects the coping process.

2.4 Coping

In a distinction from PMT, TTAT also proposes that threat appraisal, which is an amalgam of the perceptions of severity and likelihood of threats, is the primary cognitive process that is entered into to determine responses to IT mal-events, with the perceptions of the avoidability of the threat being a secondary cognitive process - "the perception that a threat exists is a necessary condition for seeking coping methods" (Liang and Xue, 2009). This proposition is also assumed in our research model.

It is when addressing the coping process itself that the real extension to PMT is derived. Coping theory suggests that "when stressful conditions are viewed as refractory to change, emotion focused coping predominates; when they are appraised as controllable by action, problem focused coping predominates" (Lazarus, 1993). Emotion focused coping is sometimes viewed as not really coping at all, but is in fact a means of adjusting perceptions of either threat or desires by developing a false perception of the environment, so that emotions related to the threat are mitigated. As Lazarus (1993) further elaborates "there is ample evidence that under certain conditions - particularly, those in which nothing useful can be done to change the situation - rational problem-solving efforts can be counterproductive".

This extension to PMT has been included in our study, to examine two potential phenomena. The first is the situation where firms perceive significant and serious security concerns in cloud adoption but decide to proceed on the basis that the risks are unavoidable. The second phenomenon is where CSC and its resulting cognitions are ignored entirely and a firm's adoption decision is based on the two other factors affecting the coping process: social influence and self-efficacy.

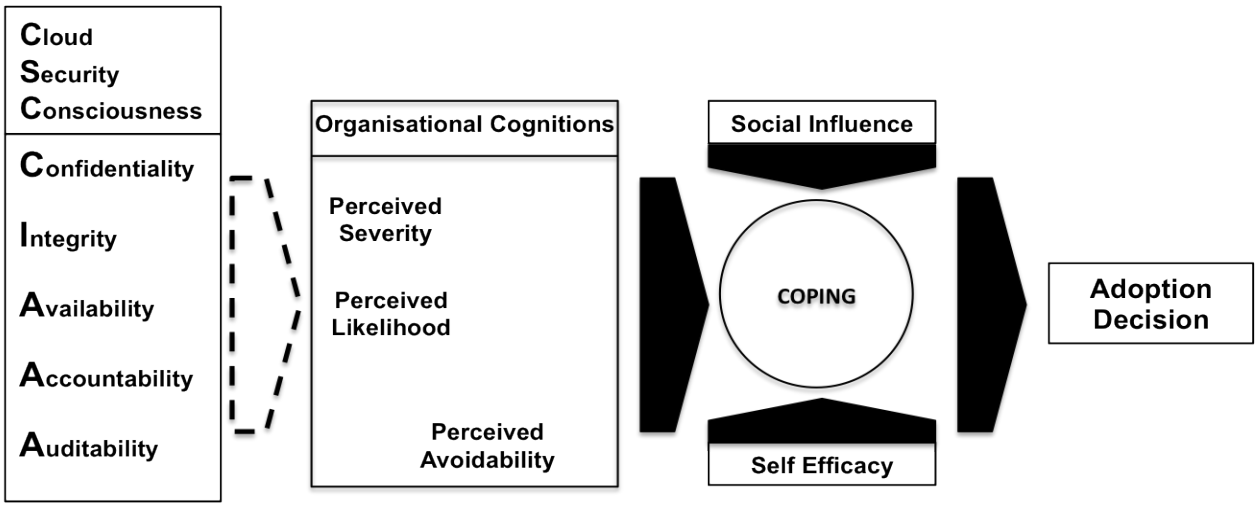
Social influence is significant in all aspects of human behaviour with one of the most pervasive determinants of a person's behaviour being the influence of other people (Burnkrant and Cousineau, 1975). In an early study, Deutsch and Gerard (1955) identified two types of social influence, 'normative' and 'informational', and described them as influences to (a) conform with the positive expectations of another and (b) to accept information obtained from another as evidence of reality, respectively. Social

influence according to Kelman (2006) occurs through three processes: compliance, internalisation and identification. In practical cloud adoption terms compliance can be said to occur when firms accept influence from others in order to garner a favourable response from customers or suppliers. Identification can be said to occur, for example, when the firm accepts influence in order to emulate the company that advises it and internalisation can be said to occur when they view another company's approach to cloud adoption as correct and take their view on board, without question. The significance of social influence has previously found particular favour in the information systems literature in relation to technology acceptance (Taylor and Todd, 1995, Venkatesh and Davis, 2000, Venkatesh et al., 2003, Pavlou and Fygenson, 2006).
In an organisational context, theorists point to the fact that social influence alone may not be enough to effect change in behaviour because of organisational inertia (the tendency to resist change and influence), a concept that cannot be properly addressed without considering organisational capabilities or efficacies (Larsen and Lomi, 2002) and therefore to complete the framework we include the notion of self-efficacy. Most models that are underpinned by PMT contain this as a primary construct (Lee and Larsen, 2009, Rippetoe and Rogers, 1987, McMath and Prentice-Dunn, 2005, Grothmann and Reusswig, 2006) with the popularity of the notion itself owing much to the work of Bandura (1977) who established a model of behavioural change underpinned by it. In an organisational setting, self-efficacy is particularly relevant because resiliency in self-efficacy is deemed essential for effective functioning due, in part, to the fact that accomplishments in business are rarely achieved through quick successes and may require more than one attempt (Bandura and Wood, 1989). This leads us to our final propositions:

P3: Social influence affects the coping process in small firms

P4: Self-efficacy affects the coping process in small firms

P5: Coping processes will result in an adoption decision (even if that is to do nothing)



* Dotted line indicates that the proposition should, but may not always, materialise

Figure 1. Proposed Conceptual Framework

3.0 Research Approach

Exploratory discussions have already taken place with six companies, four being non-IT companies that fit within the medium and small subsets of the SME classification, and two being companies engaged in the provision of IT services for small companies. Their opinions, and particularly those of the IT service providers, on the reasons for cloud services adoption could best be described as dichotomous, and as such have provided additional motivation for this study.

It is now proposed to conduct a pilot study comprising of a series of semi-structured face-to-face interviews to examine the propositions contained in this framework. This technique is suited to exploratory research, where the interview subject is often a participant in "sense making" rather than simply a source of information (DiCicco-Bloom and Crabtree, 2006). The interviews will be complemented by the inclusion of a series of vignettes, with particular reference to the coping process. Introducing vignettes makes interviews less intimidating for the subject in sensitive matters and allows behaviour which may have an ethical or subjective dimension to be measured prospectively (Siponen and Vance, 2010, Gattiker and Kelley, 1999). This segment of the research will be conducted over a two-month period beginning in March / April 2014 and will have a constituency comprising of principals of ten small firms in Ireland, with a mix of companies to include those that have previously adopted some cloud services.

4.0 Next Steps

This paper constitutes part of a research in progress aimed at understanding attitudes and behaviours of small firm principals in dealing with cloud adoption security considerations.

On a practical level, we are currently developing and refining the data collection instrument. Specifically this involves the preparation of a matrix containing cloud deployment and service models mapped against the CSC considerations (discussed in section 2.2 above), which will then be used to buttress the structured element of the semi-structured interviews.

While various aspects of the framework have been examined in prior work, they have not previously been considered in their totality as presented in this paper and never in the context of small firms, who are distinguishable from larger firms in the way that they behave. The framework in its present guise constitutes a process-oriented view of cognitions in cloud adoption and delineates how the adoption decision is progressed. However to further understand companies' behaviour in this regard it is anticipated that the framework will be reconstituted as a variance model of the process, depending on what aspects of the current framework gain traction in the initial interviews.

When complete the research will make a several contributions to the field. Firstly, it will make a contribution to the existing literature on adoption of cloud services, in that the framework will provide a lens for analysing cloud-computing adoption behaviours. Secondly, it will serve as a basis for the preparation of a series of guidelines to be followed by small firms in adopting new technologies such as cloud services.

5.0 Limitations and challenges

The limitations of this paper in its present form include its lack of empirical data and it is in remedying this that the greatest challenge presents itself. SMEs are by definition hugely heterogeneous and thus the pilot study will seek to establish some common ground in terms of behaviour patterns and attitudes in a real-world setting. It is when generalising these findings in a more extensive manner that the real challenges present themselves but this is not a reason to avoid proceeding with the study. In fact Lee and Baskerville (2003) point to Hume's truism, that *a theory may never be scientifically generalized to a setting where it has not yet been empirically tested and confirmed* and

therefore the purpose of this study is to take initial steps in that direction, for motives already outlined in the earlier sections of this paper.

References

ANTHES, G. 2010. "Security in the Cloud," Communications of the ACM (53:11), Nov, pp 16-18.

ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A. D., KATZ, R., KONWINSKI, A., LEE, G., PATTERSON, D., RABKIN, A., STOICA, I. & ZAHARIA, M. 2010. "A View of Cloud Computing," Communications of the ACM (53:4), Apr, pp 50-58.

BAARS, T. & SPRUIT, M. 2012. "Analysing the Security Risks of Cloud Adoption Using the SeCA Model: A Case Study," Journal of Universal Computer Science (18:12), 2012, pp 1662-1678.

BANDURA, A. 1977. "SELF-EFFICACY - TOWARD A UNIFYING THEORY OF BEHAVIORAL CHANGE," Psychological Review (84:2), pp 191-215.

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), May, pp 805-814.

BHATTACHERJEE, A. 2002. "Individual trust in online firms: Scale development and initial test," Journal of Management Information Systems (19:1), Sum, pp 211-241.

BURNKRANT, R. E. & COUSINEAU, A. 1975. "INFORMATIONAL AND NORMATIVE SOCIAL INFLUENCE IN BUYER BEHAVIOR," Journal of Consumer Research (2:3), 1975, pp 206-215.

CHEN, J., WANG, Y. & WANG, X. 2012. "On-Demand Security Architecture for Cloud Computing," Computer (45:7), Jul, pp 73-78.

CHONKA, A., XIANG, Y., ZHOU, W. & BONTI, A. 2011. "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," Journal of Network and Computer Applications (34:4), Jul, pp 1097-1107.

CSA 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. *In:* BRUNETTE, G. & MOGULL, R. (eds.). Cloud Security Alliance.

DEUTSCH, M. & GERARD, H. B. 1955. "A study of normative and informational social influences upon individual judgement," Journal of Abnormal Psychology (51:3), 1955.

DEWALD, J. & BOWEN, F. 2010. "Storm Clouds and Silver Linings: Responding to Disruptive Innovations Through Cognitive Resilience," Entrepreneurship Theory and Practice (34:1), Jan, pp 197-218.

DICICCO-BLOOM, B. & CRABTREE, B. F. 2006. "The qualitative research interview," Medical Education (40:4), Apr, pp 314-321.

DINEV, T. & HU, Q. 2007. "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," Journal of the Association for Information Systems (8:7), Jul, pp 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.

ENDRES, A. M. & WOODS, C. R. 2006. "Modern theories of entrepreneurial behavior: A comparison and appraisal," Small Business Economics (26:2), Mar, pp 189-202.

ENISA 2009. *Cloud Computing - Benefits, Risks and Recomendations for Information Security*, European Network and Information Security Agency.

ENISA 2011. *Survey and analysis of security parameters in cloud SLAs across the European public sector*, European Network and Information Security Agency.

GATTIKER, U. E. & KELLEY, H. 1999. "Morality and computers: Attitudes and differences in moral judgments," Information Systems Research (10:3), Sep, pp 233-254.

GROTHMANN, T. & REUSSWIG, F. 2006. "People at risk of flooding: Why some residents take precautionary action while others do not," Natural Hazards (38:1-2), May, pp 101-120.

HYMAN, P. 2013. "Augmented-Reality Glasses Bring Cloud Security Into Sharp Focus," Communications of the ACM (56:6), Jun, pp 18-20.

KAUFMAN, L. M. 2009. "Data Security in the World of Cloud Computing," IEEE Security & Privacy (7:4), Jul-Aug, pp 61-64.

KAUFMAN, L. M. 2010. "Can Public-Cloud Security Meet Its Unique Challenges?," IEEE Security & Privacy (8:4), Jul-Aug, pp 55-57.

KEEN, P. G. 1991. Relevance and rigor in information systems research: Improving quality, confidence, cohesion and impact. *In:* NISSEN, H.-E., KLEIN, H. K. & HIRSCHHEIM, R. (eds.) *Information systems research: Contemporary approaches and emergent traditions*. Elsevier North-Holland, Inc.

KELMAN, H. C. 2006. Interests, relationships, identities: Three central issues for individuals and groups in negotiating their social environment. *Annual Review of Psychology*.

KSHETRI, N. 2013. "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," Telecommunications Policy (37:4-5), May-Jun, pp 372-386.

LARSEN, E. & LOMI, A. 2002. "Representing change: a system model of organizational inertia and capabilities as dynamic accumulation processes," Simulation Modelling Practice and Theory (10:5-7), Dec 15, pp 271-296.

LAZARUS, R. S. 1993. "COPING THEORY AND RESEARCH - PAST, PRESENT, AND FUTURE," Psychosomatic Medicine (55:3), May-Jun, pp 234-247.

LEE, A. S. & BASKERVILLE, R. L. 2003. "Generalizing generalizability in information systems research," Information Systems Research (14:3), Sep, pp 221-243.

LEE, Y. & LARSEN, K. R. 2009. "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," European Journal of Information Systems (18:2), Apr, pp 177-187.

LEVY, M., POWELL, P. & YETTON, P. 2001. "SMEs: aligning IS and the strategic context," Journal of Information Technology (16:3), Sep, pp 133-144.

LIANG, H. & XUE, Y. 2009. "AVOIDANCE OF INFORMATION TECHNOLOGY THREATS: A THEORETICAL PERSPECTIVE," MIS Quarterly (33:1), Mar, pp 71-90.

LIANG, H. & XUE, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," Journal of the Association for Information Systems (11:7), 2010, pp 394-413.

MARSTON, S., LI, Z., BANDYOPADHYAY, S., ZHANG, J. & GHALSASI, A. 2011. "Cloud computing - The business perspective," Decision Support Systems (51:1), Apr, pp 176-189.

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), Mar, pp 621-643.

MELL, P. & GRANCE, T. 2011. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145 ed. Gaithersburg, MD 20899-8930.

MISRA, S. & KUMAR, E. S. 2000. "Resourcefulness: A Proximal Conceptualisation of Entrepreneurial Behaviour," Journal of Entrepreneurship (9:2), September 1, 2000, pp 135-154.

MITCHELL, R. K., BUSENITZ, L., LANT, T., MCDOUGALL, P. P., MORSE, E. A. & SMITH, J. B. 2002. "Toward a theory of entrepreneurial cognition: Rethinking the people side of entrepreneurship research," Entrepreneurship theory and practice (27:2), pp 93-104.

MODI, C., PATEL, D., BORISANIYA, B., PATEL, A. & RAJARAJAN, M. 2013. "A survey on security issues and solutions at different layers of Cloud computing," Journal of Supercomputing (63:2), Feb, pp 561-592.

NEISSER, U. 1967. *Cognitive Pyschology,* New York, Appleton-Century-Crofts.

PAVLOU, P. A. & FYGENSON, M. 2006. "Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior," MIS Quarterly (30:1), Mar, pp 115-143.

PETERSON, G. 2010. "Don't Trust. And Verify A Security Architecture Stack for the Cloud," IEEE Security & Privacy (8:5), Sep-Oct, pp 83-86.

REBOLLO, O., MELLADO, D. & FERNANDEZ-MEDINA, E. 2012. "A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment," Journal of Universal Computer Science (18:6), 2012, pp 798-815.

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), Mar, pp 596-604.

RISTENPART, T., TROMER, E., SHACHAM, H. & SAVAGE, S. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. Proceedings of the 16th ACM conference on Computer and communications security, 2009. ACM, 199-212.

ROGERS, R. W. 1975. "PROTECTION MOTIVATION THEORY OF FEAR APPEALS AND ATTITUDE-CHANGE," Journal of Psychology (91:1), 1975, pp 93-114.

SEHGAL, N. K., SOHONI, S., XIONG, Y., FRITZ, D., MULIA, W. & ACKEN, J. M. 2011. "A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing," IETE Technical Review (28:4), Jul-Aug, pp 279-291.

SHEPHERD, D. A. & KRUEGER, N. F. 2002. "An Intentions–Based Model of Entrepreneurial Teams' Social Cognition*," Entrepreneurship Theory and Practice (27:2), pp 167-185.

SIPONEN, M. & VANCE, A. 2010. "NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS," MIS Quarterly (34:3), Sep, pp 487-502.

SOOD, S. K. 2012. "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications (35:6), Nov, pp 1831-1838.

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), Jan, pp 1-11.

TAKABI, H., JOSHI, J. B. D. & AHN, G.-J. 2010. "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy (8:6), Nov-Dec, pp 24-31.

TALBOT, D. 2010. "Security in the Ether," Technology Review (113:1), pp 36-42.

TAYLOR, S. & TODD, P. A. 1995. "UNDERSTANDING INFORMATION TECHNOLOGY USAGE - A TEST OF COMPETING MODELS," Information Systems Research (6:2), Jun, pp 144-176.

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

VAQUERO, L. M., RODERO-MERINO, L. & MORAN, D. 2011. "Locking the sky: a survey on IaaS cloud security," Computing (91:1), Jan, pp 93-118.

VENKATESH, V. & DAVIS, F. D. 2000. "A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies," Management Science (46:2), Feb, pp 186-204.

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), Sep, pp 425-478.

WANG, Q., WANG, C., REN, K., LOU, W. & LI, J. 2011. "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems (22:5), May, pp 847-859.

WEST, G. P. 2007. "Collective cognition: When entrepreneurial teams, not individuals, make decisions," Entrepreneurship Theory and Practice (31:1), Jan, pp 77-102.

WESTHEAD, P., UCBASARAN, D. & WRIGHT, M. 2005. "Experience and cognition - Do novice, serial and portfolio entrepreneurs differ?," International Small Business Journal (23:1), Feb, pp 72-98.

XIAO, Z. & XIAO, Y. 2013. "Security and Privacy in Cloud Computing," IEEE Communications Surveys and Tutorials (15:2), 2013, pp 843-859.

ZISSIS, D. & LEKKAS, D. 2012. "Addressing cloud computing security issues," Future Generation Computer Systems-the International Journal of Grid Computing and Escience (28:3), Mar, pp 583-592.