



## **UWL REPOSITORY**

**repository.uwl.ac.uk**

Information security and its impact on online user behaviour: open research questions in social media business model

Tennakoon, Hemamali, Ezingear, Jean-Noel and Benson, Vladlena ORCID: <https://orcid.org/0000-0001-5940-0525> (2011) Information security and its impact on online user behaviour: open research questions in social media business model. In: The 2nd Annual Faculty of Business and Law Conference: Emerging Issues in Business and Law, 10 May 2011, Kingston upon Thames, UK. (Unpublished)

**This is the Accepted Version of the final output.**

**UWL repository link:** <https://repository.uwl.ac.uk/id/eprint/3884/>

**Alternative formats:** If you require this document in an alternative format, please contact: [open.research@uwl.ac.uk](mailto:open.research@uwl.ac.uk)

### **Copyright:**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

**Take down policy:** If you believe that this document breaches copyright, please contact us at [open.research@uwl.ac.uk](mailto:open.research@uwl.ac.uk) providing details, and we will remove access to the work immediately and investigate your claim.

### Abstract

Steady growth of e-business and reliance on technology have lead to corporate and personal information becoming valuable assets (e.g. Gordon et al., 2010). However just as any other assets, protecting information has also become a cause of concern. Information security breaches are on the rise while e-business and individual online users are subject to losses and other negative impacts of the Internet threats ( e.g. Smith et al., 2010; Campbell et al., 2003; Cavusoglu et al., 2004). The focus of this paper is to provide an overview of current research on information security constructs, factors affecting online behaviour and formation of trust in online transactions. Some open questions forming a gap in extant research conclude the paper and call for further empirical evidence. Based on an extensive literature review, as well as using secondary sources of trade publications and news reports, key concepts of information security has been identified. The deductive approach will be used where based on theory, hypotheses can be built. These can then be tested based on observations to confirm their validity. Further empirical data collection methods will be developed and employed (both qualitative and quantitative in nature) at a later stage of the study.

### Background

The concepts of information protection and information security received significant attention, the following definition given by Kritzinger & Smith (2008, p.2) comprehensively captures aims of information security as: 'the primary goal of information security is to protect information and ensure that the availability, confidentiality and integrity of information are not compromised in any way". Some researchers have brought to light some ambiguity in the definitions of 'privacy' and 'security'. According to (Bergeron, 2000) these two terms have been used as a single concept while in reality these are two separate, yet inter-related terms. Two main categories of online behaviour can be observed in literature: online buying behaviour (Miyazaki & Fernandez, 2001; Chen & Barnes, 2007; McKnight et al., 2002; Parasuraman & Zinkhan, 2002; Ranganathan & Ganapathy, 2002) and online information disclosure behaviour (Fogel & Nehmad, 2009; Hoffman et al., 1999). However, significant issues such as protection of privacy, formation of trust and risk perception online are just starting to emerge in literature as influencing user behaviour online (see Table 1 for a brief review of key studies). Recent studies provided effective recommendations for businesses how to better protect their corporate information assets through the alignment of corporate strategy and information assurance (Ezingard et al., 2007; Ezingard & Schrire, 2007). A considerable body of recent research into online user behaviour has been conducted in traditional e-business environments (e.g. Brown & Muchira ,2004; Kini & Choobineh 1998; Liu et al 2005; Corbitt et al., 2003; George, 2002; Vijayarathay et al., 2000; Grabner-Kraeuter, 2002; Rose et al. 2010; Jarvenpaa et al., 2000 etc.).

### Discussion

Presently we are witnessing formation of new business models associated with the emergence of social media. A paradigm shift in e-business models, from traditional Internet presence to social media-based businesses, has opened a new avenue for future research in the constructs of information security online.

Several business cases that appeared in the media recently provide an evidence of security and privacy issues concerning users and businesses operating in social media driven business environments. For example:

**Case 01:** The social networking site Facebook does not allow pop-up ads but uses information in member profiles to display banner ads that might be interesting to them (Cassidy, 2006).

**Case 02:** 'Ads by Google' uses a similar approach. One might argue that this 'customized advertising' as an invasion of an individual's privacy and security. (Cassidy, 2006).

**Case 03:** Burger King launched 'Whopper Sacrifice campaign' in December 2008 on the social networking site Facebook, where they offered users a free Whopper sandwich for every 10 friends they deleted from their Facebook network. Over 20,000 users deleted nearly 234,000 of their friends in exchange for a free burger. Next month, Facebook decided to bring the campaign to a closure, claiming that it raised privacy concerns (Kaplan & Haenlein, 2010).

Review of extant literature indicates that the a number key concepts play a significant role in studying information security. Table 1 summarises some of these key concepts derived from the findings of literature review.

### Open Research Questions

As mentioned before, a large number of recent research into online user behaviour has been conducted in traditional e-business environments (e.g. Brown & Muchira ,2004; Kini & Choobineh 1998; Liu et al 2005; Corbitt et al., 2003; George, 2002; Vijayarathay et al., 2000; Grabner-Kraeuter, 2002; Rose et al. 2010; Jarvenpaa et al., 2000) and does not include a compelling account of the **implications information security for social media based business models**. Therefore there is a scope for future research in this direction.

Table 1.

Key concepts	Researcher	Domain of Application	Relationship Identified/Findings
Trust, Privacy	Brown & Muchira ,2004	E-business	lack of trust cause consumers to have privacy concerns
Risk, Trust, Online behaviour	Kini & Choobineh 1998; Liu et al 2005	E-business	'Trust' is an influencing factor that will encourage a customer to take a risk.  The degree or level of trust an individual has would be positively related to whether the individual would make an online purchase.
Privacy, Security, Perceived risk (risk Perception)	Cases ,2002	E-business	Risk of loss of privacy and the risk of loss of security of personal information relates to the amount of risk an individual is willing to take in an electronic shopping context
Risk perception, Security, Online shopping behaviour	Miyazaki & Fernandez, 2001	E-business	Higher risk perception towards security does not act as a predictor of online shopping behaviour
Privacy, Security, Trust	Liu et al.,2005	E-business	Reasonable assurance that personal information is kept secure is a dimension of privacy  Degree or level of trust is determined by the assurance of security and privacy provided by the e-vendor
Trust, Behavioural intention	Corbitt et al., 2003; George, 2002; Vijayarathay et al., 2000; Grabner-Kraeuter, 2002; Rose et al. 2010; Jarvenpaa et al., 2000	E-business	Higher levels of trust is associated with repeat visits to an e-vendor (positive behavioural intention)
Information disclosure, Security, Privacy	Fogel & Nehmad, 2009; Hoffman et al., 1999	E-business	Higher security and privacy concerns will lead to reluctance to disclose information or fabrication of information.
Trust, Privacy, Security, Online buying behaviour	Chen & Barnes, 2007; McKnight et al., 2002; Parasuraman & Zinkhan, 2002; Ranganathan & Ganapathy, 2002	E-business	Perceived website quality could create a feeling of trust in terms of privacy and security and will encourage positive purchase intention.
Individual technical competencies, Trust	Connolly & Bannister, 2006	E-business	Higher level of technical efficacy in an individual could influence the of web vendor trustworthiness

### Future Research Directions

Use of social media, especially for business purposes, raises the questions of how security concerns affect the information disclosure online and what information can be considered public and what can be considered as private when it comes to disclosing information online. It has surfaced that users lack an understanding of the implication of self-declared information and casually unprotected personal data on social media (Benson, 2011). The question of **how online buying behaviour is affected by security concerns in social media-based business models** are still open to researchers.

Some researchers argued that "cultural differences seem to play a role in determining what information is transmitted, who receives the information, and ....issues of personal privacy, workplace privacy, ...also vary from culture to culture" (Zakaria et al., 2003, p.11). Therefore this research aims to identify relationships between information security and online behavior in the **context of social media based business environment in a cross cultural setting**.

### Bibliography

- Benson, Vladlena (2011) Public and private dichotomy: social networking in higher education. In: Business & Economics Society International Conference, U.S.
- Bergeron, E. (2000) The Difference Between Security and Privacy. Joint Workshop on Mobile Web Privacy WAP Forum & World Wide Web Consortium, 7-8 December 2000, Munich, Germany. [Online] <http://www.w3.org/PSP/mobile-privacy-wspapers/cks.html> [Accessed: 23/03/2011]
- Brown, M. and Muchira, R. (2004) 'Investigating the relationship between Internet privacy concerns and online purchase behavior', *Journal of Electronic Commerce Research*, 5 (1), pp. 62-70.
- Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003) 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market', *Journal of Computer Security*, 11(3), pp. 431-448.
- Cases, A.-S. (2002) 'Perceived risk and risk-reduction strategies in Internet shopping', *International Review of Retail, Distribution and Consumer Research*, 12, pp. 375-394.
- Cassidy, J. (2006) 'We media: How hanging out on the Internet became big business', *The New Yorker*, 82 (13).
- Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers', *International Journal of Electronic Commerce*, 9 (1), pp. 69-104.
- Chen, Y. H. and Barnes, S. (2007) 'Initial trust and online buyer behaviour', *Industrial Management & Data Systems*, 107 (1), pp. 21-36.
- Connolly, R. and Bannister, F. (2006) Factors influencing Irish consumers' trust in internet shopping. *Journal of Information Technology*, 22 (2), pp. 102-118.
- Corbitt, B.J., Thanasankit, T. and Yi, H. (2003) Trust and e-commerce: a study of consumer perceptions. *Electronic Commerce Research and Applications*, 2, pp. 203-215.
- Ezingard, J. N., McFadzean, E. and Birchall, D. (2007) 'Mastering the art of corroboration: A conceptual analysis of information assurance and corporate strategy alignment', *Journal of Enterprise Information Management*, 20 (1), pp. 96-118.
- Ezingard, J.N. and Schrire, M.B. (2007). Triggers of change in information security management practices, *Journal of General Management*, Vol. 32 No. 4, 53-72.
- Continued....