Information Security and its Impact on Online User Behavior: Open Research Questions in Social Media Business Model

Hemamali Tennakoon, Jean-Noel Ezingeard and Vladlena Benson, Faculty of Business and Law, Kingston University, email: k1104954@kingston.ac.uk

Abstract

Steady growth of e-business and reliance on technology have lead to personal and corporate 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 have 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 Kitzinger & Smith (2008, p.2) commercializes the aim 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’. For example: (Berenson, 2000) the 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) 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 (Ezingeard et al., 2007; Ezingeard & Schrire, 2007). A considerable body of recent research into online user behaviour has been conducted in traditional e-business environments (e.g. Brown & Muchina, 2004; Kni & Choobineh 1998; Liu et al 2005; Corbitt et al., 2003; George, 2002; Vijayasarthathy et al., 2000; Grabner-Krauter, 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 venue 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-based 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 number of 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 & Muchina 2004; Kni & Choobineh 1998; Liu et al 2005; Corbitt et al., 2003; George, 2002; Vijayasarthathy et al., 2000; Grabner-Krauter, 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.

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 'private'. Therefore there is a scope for research into online user behaviour has been conducted in traditional e-business (Berenson, 2000; 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).

As per Table 1, the degree or level of trust an individual would make an online purchase is determined by the assurance of security and privacy provided by the e-vendor.

Privacy, Security, Perceived risk (trust or risk perception) 

Risk perception, Security, Privacy

Information disclosure, Security, Privacy

Privacy, Security, Trust

Trust, Behavioural intention

Information disclosure, Security, Privacy

Privacy, Security, Trust

Trust, Behavioural intention

Individual technical competencies, Trust

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, Trust, Online behaviour

Risk, Trust, Online behaviour

Privacy, Security, Perceived risk (risk perception)

Privacy, Security, Trust

Risk, Trust, Online behaviour

Privacy, Security, Perceived risk (risk perception)

Privacy, Security, Trust

Risk, Trust, Online behaviour

Privacy, Security, Perceived risk (risk perception)

Privacy, Security, Trust

Risk, Trust, Online behaviour

Privacy, Security, Perceived risk (risk perception)

Privacy, Security, Trust

Table 1.

<table>
<thead>
<tr>
<th>Key concepts</th>
<th>Researcher</th>
<th>Domain of Application</th>
<th>Relationship Identified/Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust, Privacy</td>
<td>Brown &amp; Muchina, 2004</td>
<td>E-business</td>
<td>lack of trust causes consumers to have privacy concerns</td>
</tr>
<tr>
<td>Risk, Trust, Online behaviour</td>
<td>Kini &amp; Choobineh, 1998; Liu et al, 2005</td>
<td>E-business</td>
<td>&quot;Trust&quot; is an influencing factor that will encourage a customer to take a risk</td>
</tr>
<tr>
<td>Privacy, Security, Perceived risk (trust or risk perception)</td>
<td>Causes, 2002</td>
<td>E-business</td>
<td>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</td>
</tr>
<tr>
<td>Risk perception, Security, Online shopping behaviour</td>
<td>Miyazaki &amp; Fernandez, 2001</td>
<td>E-business</td>
<td>Higher risk perception towards security does not act as a predictor of online shopping behaviour</td>
</tr>
<tr>
<td>Privacy, Security, Trust</td>
<td>Liu et al, 2005</td>
<td>E-business</td>
<td>Reasonable assurance that personal information is kept secure is a dimension of privacy</td>
</tr>
<tr>
<td>Risk perception, Security, Online shopping behaviour</td>
<td>Miyazaki &amp; Fernandez, 2001</td>
<td>E-business</td>
<td>Degree or level of trust is determined by the assurance of security and privacy provided by the e-vendor</td>
</tr>
<tr>
<td>Trust, Behavioural intention</td>
<td>Corbitt et al., 2003; George, 2002; Chen &amp; Barnes, 2007; McKnight et al., 2002; Parasuraman &amp; Zinkhan, 2002; Ranganathan &amp; Ganapathy, 2002</td>
<td>E-business</td>
<td>Higher levels of trust is associated with repeat visits to an e-vendor (positive behavioural intention)</td>
</tr>
<tr>
<td>Information disclosure, Security, Privacy</td>
<td>Fogel &amp; Nehmad, 2009; Hoffman et al., 1999</td>
<td>E-business</td>
<td>Higher security and privacy concerns will lead to reluctance to disclose information or fabrication of information.</td>
</tr>
<tr>
<td>Trust, Privacy, Security, Online buying behaviour</td>
<td>Chen &amp; Barnes, 2007; McKnight et al., 2002; Parasuraman &amp; Zinkhan, 2002; Ranganathan &amp; Ganapathy, 2002</td>
<td>E-business</td>
<td>Perceived website quality could create a feeling of trust in terms of privacy and security and will encourage positive purchase intention.</td>
</tr>
<tr>
<td>Individual technical competencies, Trust</td>
<td>Connolly &amp; Bannister, 2006</td>
<td>E-business</td>
<td>Higher level of technical efficacy in an individual could influence the of web vendor trustworthy</td>
</tr>
</tbody>
</table>