Testing a Model of Users' Web Risk Information Seeking Intention

Lixuan Zhang
Georgia Regents University, Augusta, GA, USA
gzhang@gru.edu

Robert Pavur
University of North Texas, Denton, TX, USA
robert.pavur@unt.edu

Paul York
Georgia Regents University, Augusta, GA, USA
pyork@gru.edu

Clinton Amos
Weber State University, Ogden, UT, USA
clint.amos@gmail.com

Abstract

This study aims to understand the web risk information seeking intention of end users. Applying the risk information seeking and processing model (RISP), this paper examines end users' web risk information seeking intention. Hypotheses are proposed concerning the intention to seek information about one emerging web risk: cross site scripting. Data were collected from 201 college students in the southern United States. The results suggest that information insufficiency, informational subjective norm, and affective response are positively related to web risk information seeking intention. In addition, informational subjective norm and negative affect are positively related to information insufficiency. Negative affect is determined by perceived vulnerability and perceived severity of the web risk. The study proves RISP to be an adequate model to use in the web risk context and provides an enriched understanding about users' intention to seek web risk information.

Keywords: communication effectiveness, computer crime, web risk, information security

Introduction

Evolved from a mere catalog tool, the web now has become a platform for electronic commerce, social networking, entertainment, and much more; however, more aggressive risks appear with increasing web functionalities (Waldow & Gorelik, 2009). Many forms of malicious web attacks can cause great damage to individuals as well as organizations. According to a security study conducted between January 1st, 2006, and August 25th, 2010 (WhiteHat Security, 2011), the average website has thirteen serious unresolved vulnerabilities. The worst industries are Information Technology, Retail, and Education with an average of 24, 17, and 17 serious vulnerabilities per website, respectively. With these alarming numbers of vulnerabilities, end users may face the danger of disclosing their credit card number,

Editor: Kay Fielden

social security number, personal health information, and other private information. To prevent potential losses, end users should actively seek information about web risks to learn how to cope with them. In this paper, risk is defined as things, forces, or circumstances that pose danger to people or to what they value (Stern & Fineberg, 1996).

Much research has been conducted on end user security. However, there are several gaps that need to be addressed. First, there is a paucity of research on users' web risk information seeking. Researchers often focus on attitude towards the risks or protective intention, but this stream of research pays little attention to the mechanism that occurs during users' risk information seeking process. Second, most research has targeted traditional security risks such as spyware or viruses in email attachments (Dinev & Hu, 2007; Ng, Kankanhalli, & Xu, 2009). New emerging web risks have not been investigated. Crimes on the web today are very different from the traditional network attacks. The browsers have become increasingly complex with access to more powerful scripting tools and external plug-ins, attracting more stealthy attacks (Provos, Rajab, & Mavrommatis, 2009).

The article intends to address one question: What motivates a user to actively seek web risk information? To answer the question, the study draws from communication research and adapts the risk information seeking and processing model (RISP) to predict users' intention to actively seek web risk information. The paper is organized as follows: first, RISP and the new risks on the web are detailed. Next, the survey methodology is described and the results are analyzed. Finally, academic and practical implications of this research are explored.

Literature Review

Risk Information Seeking

The risk information seeking and processing model (RISP) was proposed by Griffin, Dunwoody, and Neuwirth (1999). Adapted and synthesized from the Heuristic-Systematic Model (HSM) (Eagly & Chaiken, 1993) and the Theory of Planned Behavior (TPB) (Ajzen & Fishbein, 1980), the model intends to predict the extent to which a person seeks out the risk information and the extent to which he or she will spend time and effort analyzing the risk. The previous risk communication paradigm adopts a top-down approach; that is, the general public relies on institutions, industries, and experts for risk management. The assumption is that people do not have sufficient knowledge and capability to judge risks. Therefore, the risk communication messages are based on experts' conceptualization of these risks. The major drawback of this approach is that it ignores the role of the people who are ultimately exposed to the risks. Therefore, the message conveying risk information may be incomprehensible to the general public.

The RISP model adopts a bottom-up approach that indicates that the information providers should take into consideration the general public's information needs and perception. People are more likely to seek and process information when the information is perceived as important, useful, and relevant. Rather than asking how messages may influence people, the bottom-up approach focuses on how people evaluate risks, make reasonable choices, and develop changes in their attitude and behaviors. Crafted this way, messages communicating risks may produce a more profound effect on people's risk-related attitude and behavior.

The RISP model posits that a person's risk information seeking intention or behavior is affected by information sufficiency, perceived information gathering capacity, and relevant channel belief (Griffin et al., 1999). The concept of information sufficiency follows the HSM's assumption of validity seeking motive and describes the confidence that one wants to have in one's knowledge about a risk will affect the risk information seeking intention. Perceived information gathering capacity reflects one's perceived ability to gather and locate relevant risk information. Relevant

channel beliefs relate to the individual's trust and perceived usefulness about the information source that delivers the message. People can get Internet risk information from multiple channels, including newspaper, magazines, websites, social media, and other people. The beliefs about each media channel will be formed based on the perceived quality of information of each channel as well as the search cost. However, this portion of the model is still exploratory (Griffin et al., 2006).

Another notable RISP component is informational subjective norms, which originates from Ajzen's (1991) concept of subjective norm in theory of planned behavior (TPB). The informational subjective norms refer to the perceived social influences affecting one's perception about the knowledge he or she should have. RISP proposes that the informational subjective norms will affect the information sufficiency. An additional TPB component used in the RISP model is perceived behavioral control, which is labeled as perceived information gathering capacity.

The RISP model also incorporates perceived hazard characteristics and affective responses to risk. Risk judgment is considered multidimensional and includes several hazard characteristics such as risk severity, risk vulnerability, risk immediacy, and risk benefits. In the RISP model, perceived hazard characteristics affect affective responses. Emotional aspects of risk perception such as worry, fear, dread, or outrage are strongly related to perceived hazard characteristics (Witte, 1992). Affective responses also affect the judgmental confidence and motivate information seeking and processing more than the cognitive component of risk perception.

Scholars have applied this model in investigating industrial risks (Huurne & Gutteling, 2005; B. B. Johnson, 2005), environmental risks (Kahlor, 2007; Kahlor, Dunwoody, Griffin, & Neuwirth, 2006), and food risks (Kuttschreuter, 2006), and the support for the model has been quite strong. Recently the robustness of the RISP model has been validated by two ways: a report of a comparative analysis across five risks and a review of literature that has utilized at least some of the RISP model (Griffin, Dunwood, & Yang, 2012). However, current research has not incorporated this model to explain web risk information seeking behavior. Much research has explored users' perception of online risks and how it may influence their behavior on the Internet; how users seek web risk information remains to be studied.

Risks on the Web

The web is a very open platform, where new technologies enable a combination of content and services from multiple sources. Users today expect the web to be sophisticated, functional, and easy to navigate. However, the complex architecture of the web also leads to new types of vulnerabilities. Most browsers tolerate malformed inputs so attacks may succeed despite appearing abnormal. For example, SQL injection occurs when a database query is inserted into a web form input box to gain access to data or make changes to the data. In addition, browser cookies, the mechanism for storing user or session information, are susceptible to theft, forgery, and hijacking. Common website vulnerabilities include cross site scripting (XSS), information leakage, content spoofing, and SQL injection. Among all the vulnerabilities, cross-site scripting is the most prevalent website vulnerability, identified in over 71% of all websites (Grossman, 2010). This study will focus on XSS.

Cross-site scripting was first reported in an advisory from Carnegie-Mellon University's CERT Coordination Center (CERT, 2000), XSS is an attack in which scripting code is injected into the web pages generated by web applications. This potentially malicious code executes in a user's browser when the page is accessed. According to Grossman (2010) there are two types of XSS attacks: persistent XSS attacks and non-persistent XSS attacks. In a persistent attack, hackers submit XSS exploit code as part of a free-form text input such as a comment or a product review. The actual attack happens when a future visitor requests to view this text. Rather than being dis-

played to the visitor, as would the text of a traditional comment or review, the script code (referred to as the "payload") is executed, often without the visitor even being aware of its execution. In a non-persistent attack, the exploit code is not stored persistently on a web site. Instead, it is encoded as part of the universal resource locator (URL) used to access a dynamically created page. When the page is accessed, the script payload is rendered along with the page and the script code is executed. XSS infected URLs can be distributed through email messages, discussion board posts, or any number of other media channels.

Most types of conventional security measures such as firewalls, virus protection software, and intrusion detection systems cannot do much to detect or protect against XSS attacks. These attacks do not require a web application developer to be intentionally malicious and often exploit otherwise trustworthy web sites. The attacks are enabled by web application developers' lack of security awareness or programming mistakes. To prevent XSS attacks, developers need to perform solid data input validation on user-submitted content and only accept expected characters in the appropriate data format.

Many companies have been victims of XSS worms. In 2005, MySpace was hit by an XSS worm which infected over one million users' profiles within 20 hours of the initial infection. MySpace was forced to shut down to fix the problem after two days. Twitter has suffered from four variants of an XSS attack, hijacking users' account and advertising the hacker's website by posting tweets on behalf of account holders.

Hypothesis Development

Based on the RISP model, a web risk information seeking and processing model is proposed in Figure 1. Two components, informational subjective and perceived information gathering ability, are maintained in full from the original RISP model. Affective response is relabeled as negative affect since the emotional reactions towards risks are mainly negative. In this paper, information insufficiency is used instead of information sufficiency to clearly indicate the gap between de-

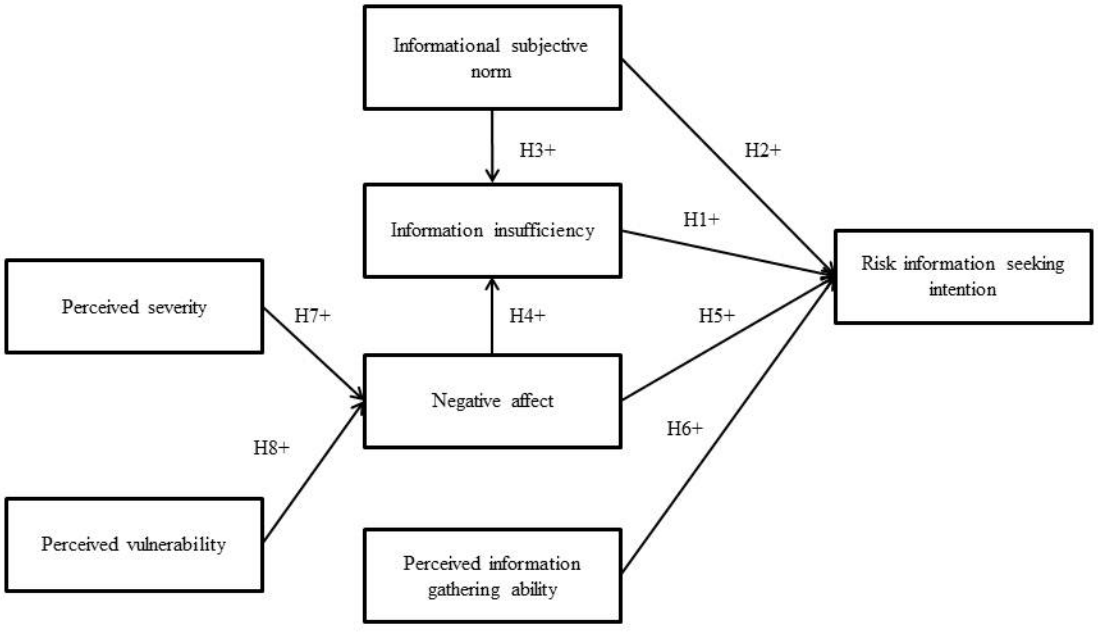

Figure 1: Research model

sired confidence and perceived confidence in one's knowledge about risk. For the component perceived hazards characteristics, two dimensions of risk perception are examined: perceived severity and perceived vulnerability. The component perceived channel belief is not included since the portion of the model is still exploratory (Griffin et al., 2006). The dependent variable web risk information seeking intention is defined as individuals' intention to seek information about web risks.

Information Insufficiency

Information insufficiency is defined as the perceived size of the gap between the information held and information needed that will affect the information seeking behavior about a certain risk (Kahlor, 2007). As a central concept in RISP, it suggests that each individual has a different quantity of information requirements that he or she considers as necessary to deal with a risk. The concept originates from Eagly and Chaiken's (1993) notion of "sufficiency threshold". Eagly and Chaiken (1993) defined sufficiency threshold as the receiver's desired level of confidence about a risk. The receivers are often guided by the principle of least effort. That is, they often exert as little effort as necessary to close the gap between the actual and desired level of confidence. Therefore, as the discrepancy between the actual and desired level of confidence grows, motivations on active information seeking increase.

Previous studies show that users often have misconceptions of web security, including those who work in high-technology communities (Friedman, Hurley, Howe, Felten, & Nissenbaum, 2002). Users often have an incomplete or incorrect understanding of various web security technologies (Furnell & Karweni, 1999). They have tried to educate themselves regarding web security but with mixed results, largely due to the technical difficulties of the subject (Flinn & Lumsden, 2005). It is argued, however, that a user will be motivated to seek more information about web risks when they perceive a need for more information. Recent research finds that information insufficiency is related to information seeking (Kahlor, Dunwoody, Griffin, Neuwirth, & Giese, 2003). Thus:

H1: Information insufficiency is positively related to web risk information seeking intention.

Informational Subjective Norm

Originating from the concept of subjective norm (Ajzen & Fishbein, 1980), informational subjective norm refers to perceived social influence motivating the desire to be informed about a certain risk. According to the model of planned behavior, the best predictors of people's behavior are determined by two variables: individuals' own attitude towards the behavior and individuals' perception of how other people want them to behave. People tend to conform to the social pressure of what is expected from them. Therefore, web risk information seeking may have a social component. Through shared cognition, individuals may believe the security knowledge is important if their peers believe so. In addition, individuals prefer to ensure the favorable evaluation of themselves and satisfactory reactions from others. Being a victim of security breach or identify theft will bring embarrassment, which plays an important role in security-related behavior. Recent research finds that that subjective norm is influential in users' intention to engage in protective behavior (Anderson & Agarwal, 2010; Herath & Rao, 2009).

In the context of web risk information seeking, if a person's family and friends think that seeking knowledge about a risk is important, it will increase his or her desire to obtain information. The subjective norms may make people feel their information on the web risks is insufficient and drive them to actively seek and accumulate information pertaining to these risks. Studies have reported that the subjects reported a larger gap between the knowledge they had about the risk and the amount of knowledge that they felt was sufficient when others expect them to be in-

formed about a risk (Griffin et al., 1999; Kahlor, 2007; Lerner & Kelner, 2000). Therefore, the following hypotheses are proposed:

H2: Informational subjective norm is positively related to web risk information seeking intention.

H3: Informational subjective norm is positively related to information insufficiency.

Negative Affect

Affect has been incorporated into people's judgment and decision making (Lerner & Kelner, 2000; Loewenstein, Weber, Hsee, & Welch, 2001). Emotional reactions to risks are often different from the cognitive evaluations of the risks. Affective response is more rapid and basic than cognitive evaluations, providing a fast and rough assessment. Affect can also influence cognitive processing. For example, participants who are induced to feel negative affect consistently made more pessimistic estimates about a certain risk than others who were induced to feel positive affect (E. Johnson & Tversky, 1983).

When it comes to web security issues, the common affect people experience are negative emotions such as fear, worry, anger, anxiety, and frustration. Negative affect is defined as a dimension of subjective distress and unpleasant engagement that includes a variety of aversive mood states, such as worry, anger, fear, disgust, and other moods (Watson, Clark, & Tellegen, 1988). Negative affect could increase the relevance of the message and produce behavior change consistently. Many studies have found a significant relationship between negative affect and compliance with the recommended action (Sutton, 1982; Zhang & McDowell, 2009). A recent study finds that fear appeal impacts end user behavioral intentions to comply with recommended security guidelines (E. Johnson & Tversky, 1983). According to RISP, negative affect such as worries and fear could make people feel inadequate about their knowledge about the risks and motivate people to seek more information. Therefore, the following hypotheses are proposed:

H4: Negative affect is positively related to information insufficiency.

H5: Negative affect is positively related to web risk information seeking intention.

Perceived Information Gathering Capacity

Perceived information gathering capacity refers to one's perceived ability to perform the information seeking steps for the desired outcome, especially when the outcome requires effort and non-routine information gathering (Griffin et al., 1999). Seeking information about web risk requires information gathering. For example, to learn about a new web risk, an individual needs to be actively involved and gather information from different channels, such as talking with experts, researching on the Internet, and reading security news and reports. A person capable of gathering risk information is likely to spend more efforts and persistence on seeking risk information. Higher levels of perceived capacity may lead individuals to approach a task, whereas lower levels of perceived capacity may lead individuals to avoid it. Huurne (2008) found that perceived information-gathering capacity is positively associated with information seeking and negative associated with information avoidance. Thus:

H6: Perceived information gathering capacity is positively related to web risk information seeking intention.

Perceived Hazard Characteristics

RISP posits that the perceived hazard characteristics have multiple components. This study will focus on two components: perceived severity of the threat and perceived vulnerability of the threat. Perceived severity assesses how severe a person believes a threat will be to his or her life.

The more serious a person perceives a risk to be, the more likely he or she will experience negative emotions such as fear and anxiety. Web users develop a perception of threat after assessing problems in their computing environment. If they do not perceive a threat as severe, then they will not feel negative affect.

Perceived vulnerability concerns the susceptibility a person has to a threat. Even severe threats may be ignored if people think they are not vulnerable to them. People tend to believe that they are less vulnerable to risks than others. For example, most people believe they are better than the average driver and that they will live longer than average life expectancy (Slovic, Fischhoff, & Lichtenstein, 1986). Therefore it is not surprising to find that people perceive themselves at less risk of computer vulnerability than others. Users believe that only people with important information or people who have annoyed the attackers should be concerned with any computer risks (Weirich & Sasse, 2001). It is expected, however, that those individuals who do have a high degree of perceived vulnerability will be more likely to have negative emotions towards the risks. Previous research has shown that perceived vulnerability and perceived severity are positively related to perceived threat and protective intention (Lee &Larsen, 2009; Liang & Xue, 2010). Therefore, the following hypotheses are proposed:

H7: Perceived severity of the threat is positively related to negative affect.

H8: Perceived vulnerability of the threat is positively related to negative affect.

Methodology

The research model was tested with data obtained using an online survey instrument from students in two universities in southern United States. The authors have obtained the approval of the institutions' IRB for the study and the participants gave written informed consent. All students are business undergraduate students enrolled in senior-level business classes such as information systems management, healthcare marketing, operation management, and system analysis and design. They were given extra credit for taking the survey. The student sample was deemed appropriate since the study focuses on information seeking on the web and students, in general, tend to be the most active web users. Researchers have used student samples for theory testing (Lopes & Galletta, 2006), which fits the purpose of this study. In addition, as indicated in a previous study (Wang & Wallendorf, 2006), the decision-making processes of students are consistent with that of other populations. The students were presented an excerpt about XSS from a report by WhiteHat (2011). The article is about a page long with 599 words. Then they were asked to answer the questions of the survey. A total of 201 completed responses were used. Among them, 49.5% of them were males and 50.5% of them were females. 81% of them were between 20 to 29 years old. 68% of them had work experience.

All survey items were borrowed or adapted from existing scales. All constructs are measured in Likert or semantic scales except information insufficiency. Information insufficiency is measured by two items. One is current knowledge: "Rate your current knowledge about XSS on a scale of 0 to 100 where zero means knowing nothing and 100 means knowing everything you could possibly know about this topic." The other one is sufficiency threshold: "Think of that same scale again. This time we would like you to estimate how much knowledge you would need to achieve a comfortable understanding of XSS. You might feel you need the same, more, or possibly even less information about the topic. Using a scale of zero to 100, how much information would be sufficient for you?" Information insufficiency can be obtained by subtracting the current knowledge score from the sufficiency threshold score for each individual. However, this procedure can multiply reliability problems and suffer from ceiling effects. Consistent with previous studies (Kahlor et al., 2003; Yang et al., 2010), the second item was used to evaluate the impact of information insufficiency while controlling for current knowledge.

Negative affect is measured by six items using a semantic scale ranging from -2 to +2. Items include "anxious–comfortable," "tense – content" and "worried – at ease." The scale is recoded where 5 represents the most negative mood and 1 represents the most positive mood. All other constructs are measured by Likert scales ranging from 1 to 5. Informational subjective norm is measured by four items. One example item is "The people I spent most of my time with are likely to seek information related to XSS." Perceived vulnerability, perceived severity, and perceived information gathering capacity are measured by three items each. The dependent variable was measured by three items: "I plan to seek more information about XSS in the future", "I intend to find out more about XSS," and "In the future, I will try to seek as much information as I can about XSS." All items, along with their descriptive statistics are listed in the Appendix

Results

Partial Least Squares (PLS), specifically SmartPLS 2.0 (Ringle, Wende, & Will, 2005), was used to assess the psychometric properties of the measurement model and to test the hypotheses. Utilizing a component-based approach, PLS is designed to not only explain the variances, i.e., to examine the significance of the relationships and variance explained, such as in linear regression, but also to simultaneously model the structural paths and measurement paths (Gefen, Straub, & Boudreau, 2000). PLS was chosen over covariance-based Structural Equation Modeling for two reasons. First, it is not contingent upon the data having multivariate normal distributions and interval nature (Fornell & Bookstein, 1982), which makes PLS suitable for handling variable such as information insufficiency. Second, it is appropriate for testing theories in the early stages of development (Fornell & Bookstein, 1982). Although RISP has been tested in other fields, it is a relatively new theory in the context of web risk. According to Gefen, Rigdon, and Straub (2011), substantive reasons for using PLS include exploratory research objectives and ensuring convergence.

Assessment of Measurement Model

The adequacy of measurement model can be demonstrated through measures of convergent and discriminant validity. Discriminant validity of the constructs were assessed by two criteria: 1) each item should have a higher loading on its hypothesized construct than on other constructs and 2) the square root of each construct's average variance explained should be higher than its correlation with other constructs. Table 1 shows the factor loading and cross-loading results from a principal component factor analysis. Items do have much higher self-loadings than cross loadings. Then the square root of the AVE of a construct is compared with its correlation. As Table 2 indicates, the AVE's square root is greater than the cross correlations among the constructs. The construct "information insufficiency" is not included since it is measured by one item. Convergent validity is assessed by composite reliability of constructs and variance extracted. Table 1 provides reliability results. The data shows that the constructs demonstrate satisfactory internal reliability. The composite reliabilities range from 0.75 to 0.98, which exceeds the recommended value of 0.70 (Gefen et al., 2000). The average variance extracted (AVEs) are above 0.5, as recommended by Fornell and Larcker (1981).

Table 1: Cross-loading of the constructs, composite reliability and AVE						
Item	**Severity**	**Info Seeking**	**Info Gathering**	**Negative Affect**	**Subjective Norm**	**Vulnerability**
Severity1	0.85	0.45	0.31	0.31	0.42	0.54
Severity2	0.89	0.43	0.22	0.27	0.42	0.49
Severity3	0.79	0.38	0.39	0.35	0.37	0.43
InfoGather1	0.23	0.27	0.78	0.13	0.38	0.21
InfoGather3	0.28	0.26	0.83	0.10	0.46	0.20
InfoGather4	0.32	0.28	0.86	0.13	0.39	0.25
InfoSeek1	0.47	0.98	0.34	0.41	0.58	0.41
InfoSeek2	0.48	0.98	0.35	0.42	0.55	0.40
InfoSeek3	0.49	0.96	0.32	0.42	0.57	0.33
NegaAffect1	0.37	0.39	0.20	0.89	0.34	0.36
NegaAffect2	0.30	0.38	0.15	0.91	0.31	0.36
NegaAffect3	0.29	0.37	0.18	0.87	0.31	0.33
NegaAffect4	0.37	0.39	0.28	0.87	0.36	0.44
NegaAffect5	0.28	0.33	0.16	0.84	0.25	0.33
SubNorm1	0.37	0.49	0.44	0.33	0.80	0.34
SubNorm2	0.42	0.47	0.45	0.30	0.86	0.39
SubNorm3	0.46	0.52	0.42	0.31	0.81	0.43
SubNorm4	0.30	0.42	0.40	0.22	0.80	0.24
Vulnerability1	0.49	0.37	0.26	0.43	0.36	0.91
Vulnerability2	0.52	0.35	0.32	0.33	0.40	0.91
Vulnerability3	0.59	0.35	0.29	0.37	0.43	0.92
AVE	***0.71***	***0.95***	***0.51***	***0.77***	***0.67***	***0.84***
Composite reliability	***0.88***	***0.98***	***0.75***	***0.94***	***0.89***	***0.88***

Table 2: Discriminant validity of the constructs						
Construct	**1**	**2**	**3**	**4**	**5**	**6**
Perceived severity	**0.84**					
Negative affect	0.37	**0.88**				
Perceived info. gathering capacity	0.37	0.22	**0.71**			
Information seeking intention	0.50	0.43	0.35	**0.97**		
Informal subjective norm	0.48	0.36	0.52	0.58	**0.82**	
Perceived vulnerability	0.58	0.42	0.31	0.39	0.43	**0.91**
Note: The diagonal elements represents square root of AVE						

Assessment of Structural Model

With adequate measurement model, the hypotheses were tested by examining the structural model. The PLS algorithm and the bootstrapping re-sampling methods were used with the 201 cases, and 1000 re-samples were used to estimate the model. Figure 2 shows the results. The model accounts for 43% of variance in information seeking intention, 17% of variance in information insufficiency, and 20% of variance in negative affect. According to Chin (1998), R^2 values of 0.67, 0.33, or 0.19 for endogenous latent variables are described as substantial, moderate, or weak. Therefore, the variance explained in information seeking intention can be described as moderate while the variances of negative affect and information insufficiency can be described as being weak.

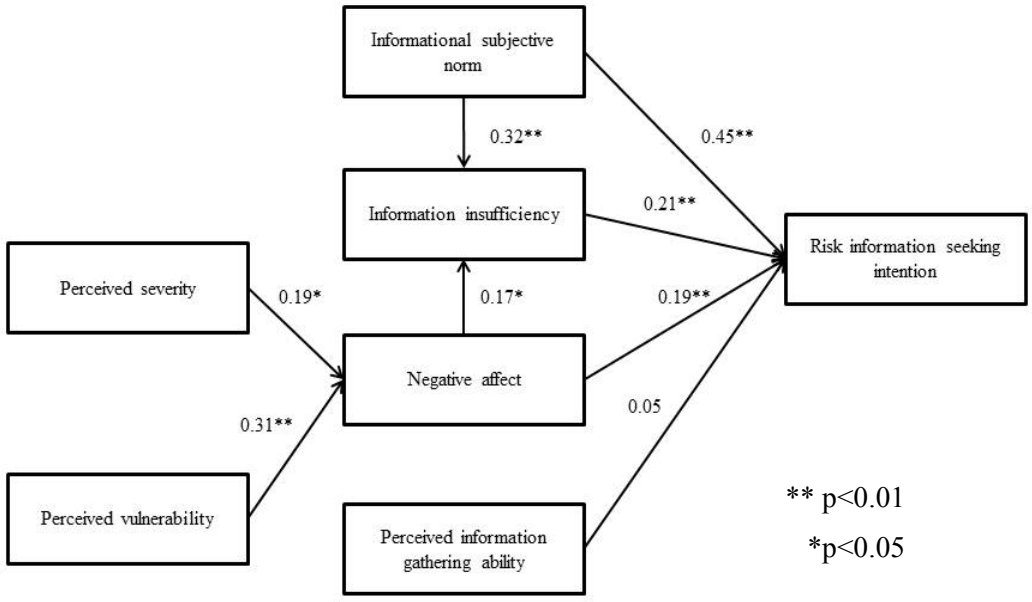

Figure 2: Model testing results

As hypothesized, information insufficiency (b=0.21, p<0.01) and informational subjective norm (b=0.45, p<0.01) are positively related to web risk information seeking intention, providing support for H1 and H2. Sufficient support is found for H3 (b=0.32, p<0.01), which hypothesized that informational subjective norm is positively related to information insufficiency. There is a signif-

icant relationship between negative effect and information insufficiency (b=0.17, p<0.05). Therefore H4 is supported. Negative affect has a significant relationship with information seeking intention (b=0.19, p<0.01), lending support to H5. The results do not reveal any significant relationship between perceived information gathering capacity and web risk information seeking intention. Therefore H6 is rejected. Negative affect is significantly determined by perceived severity (b=0.19, p<0.05) and perceived vulnerability (b=0.31, p<0.01). Thus, H7 and H8 are both supported. Table 3 summarizes the results of the study.

Table 3: Summary of results

Path	Coefficient	Std. Error	Result
Information insufficiency → intention	0.2034	0.0658	Supported
Informational subjective norm → intention	0.4469	0.0687	Supported
Informational subjective norm → information insufficiency	0.3162	0.0765	Supported
Negative affect → information insufficiency	0.1741	0.0805	Supported
Negative affect → intention	0.1935	0.0691	Supported
Perceived information gathering capacity → intention	0.0453	0.0648	Rejected
Perceived severity of the threat → negative affect.	0.1934	0.0991	Supported
Perceived vulnerability of the threat → negative affect	0.3065	0.0795	Supported

The PLS structural model is mainly evaluated by Goodness-of-Fit (GoF) (Tenenhaus, Esposito Vinzi, Chatelin, & Lauro, 2005) and by using the Stone-Geisser Q-square test for predictive relevance (Geisser, 1975; Stone, 1974). Goodness-of-Fit (GoF) (Tenenhaus et al., 2005) was employed to judge the overall fit of the model. GoF, calculated as the geometric mean of the average communality and the average R^2, representing an index for validating the PLS model globally. For this model, the GoF is 0.43 which exceeds the cut-off value of 0.36 and shows that the model performs well (Wetzels, Odekerken-Schröder, & van Oppen, 2009).

The Q-squares statistics measure the predictive relevance of the model by reproducing the observed values by the model itself and its parameter estimates. When estimating Q square, blindfolding procedure ignores a part of the data for a particular block during parameter estimation (a block of indicators is the set of measures for a construct). The ignored data part is then estimated using the estimated parameters, and the procedure is repeated until every data point has been ignored and estimated (Chin, 1998). In PLS, one type of Q-squares statistics is cross-validated redundancy. The cross-validated redundancy measures the capacity of the path model to predict the endogenous manifest variables indirectly from a prediction of their own latent variable using the related structural relation by cross-validation (Tenenhaus et al., 2005). The cross-validated redundancy measure can be a reliable measure of the predictive relevance of the model investigated (Fornell & Cha, 1994). If the redundant communality was found to be larger than 0 for all the endogenous variables, the model is considered to have predictive validity, otherwise, the predictive relevance of the model cannot be concluded (Fornell & Cha, 1994). The results of our model indicate that the cross-validated redundancies for information seeking intention, negative affect, and information insufficiency were respectively 0.39, 0.15, and 0.18. Thus the predictive validity of the used model was established.

Discussion

Overall the study shows that the RISP model can be applied in a web risk information seeking context. The model proposes four predictors of web risk information seeking intention: information insufficiency (H1), informational subjective norm (H2), negative affect (H5), and perceived information gathering capacity (H7). The results reveal that there is a strong relationship between information insufficiency and web risk information seeking intention. The larger the knowledge gap a person perceives, the stronger the intention of information seeking. The results also support the hypothesis that informational subjective norm is positively related to web risk information seeking intention. The social pressure to stay on top of web risks, such as XSS, motivates people to acquire knowledge about them. Negative affect is also significantly related to information seeking intention. The more negative emotion people experience, the stronger their information seeking intentions are. There is no significant relationship between perceived information gathering capacity and web risk information seeking intention. In this study, the participants perceived themselves capable of gathering information about XSS (mean =3.21), but that does not lead to higher likelihood of web risk information seeking.

This study also hypothesizes that informational subjective norm (H3) and negative affect (H4) are significantly related to information insufficiency. H3 is supported. The social pressure to be informed about the web risks increases the need for information. It should be noted, however, users' higher need for information does not imply that they are less knowledgeable about security issue. Interestingly, the two items measuring current knowledge and information insufficiency have a significant positive correlation. In other words, the people who rate themselves as having higher levels of knowledge about XSS also perceive higher need to acquire more information. There is also a significant relationship between negative affect and information insufficiency. Strong negative emotions experienced by an individual lead to larger perceived information insufficiency. Perceived severity (H7) and perceived vulnerability (H8) are hypothesized to be related to negative affect. Both hypotheses are supported. Negative emotions are aroused by the perceived susceptibility and severity levels of XSS.

Theoretical Implications

This study makes important contributions to the behavioral issues of seeking web risks. This is the first study drawing on RISP, providing empirical support for the cognitive process of a user's web risk seeking. As a relatively new model, RISP serves as a satisfactory model in the new context. First, the model highlights the cognitive mechanisms that occur during the web risk seeking. In particular, the results demonstrate that the information insufficiency strongly relates to web risk information seeking intention. The study also investigates the role of affective response on shaping a user's intention in seeking web risks. From the affective perspective, the results show that greater levels of perceived vulnerability and severity substantially increase emotions, which also impacts risk information seeking intention. This finding highlights the roles that affect, along with cognition, plays in an individual's desire to seek out risk information to alleviate risk perception. Finally, model testing highlights the importance of social norms for facilitating risk information seeking. This study extends research on social norms and shows that its robustness even extends to behaviors such as risk information seeking in a web context. In summary, as a bottom-up approach, RISP supports the notion that users' needs and perceptions should be taken into consideration along with social factors in modeling web risk information seeking intention.

Practical Implications

In practical terms, the results provide an enriched understanding of why users seek web risk information. The finding that informational subjective norm has a strong positive relationship with

information seeking highlights the importance of a strong organizational security culture. When employees feel the social pressure from other people for keeping updated with the security knowledge, they will be more likely to do so.

The model also suggests that affective response is related to information seeking intention. In order to motivate users to seek web risk information, the reports conveying those risks need to be presented in a way that appeals emotionally to the audience. When the audience feels emotional anxiety and fear after receiving the message, they are more likely to feel that their knowledge is inadequate. The risk-as-feeling hypothesis (Loewenstein et al., 2001) states that people respond to risks based on their emotional influences. In addition, for the messages conveyed in the articles to be emotionally appealing, they should be easily interpretable. Users may get confused if they encounter technical terms and eventually give up any further attempts at understanding the messages. Currently the majority of articles on XSS focus on the technical dimensions of the risk with software developers as the target audience. Without having end users as the target audience, these articles will not be considered relevant and useful. It is imperative to implement an end user based approach to web risk communication.

The participants had a low level of knowledge on web risks such as XSS. In this study, the current perceived knowledge is 33 on a 100 scale indicating that participants knew very little about XSS. It is imperative that individuals raise their level of awareness pertaining to these emerging risks since calls for protective action are dependent on end-users' awareness. End users' blindness to emerging web risks delays the implementation of protective actions, further confounding the security risk. Online companies, social advocacy groups, and educational institutions should allocate enough time to develop training courses for end users. Well-designed security courses can effectively raise end users' awareness and assist in speeding up the development of counteractions for addressing web security risks. Online games have been proven successful in teaching users to identify fraudulent websites and avoid phishing attack (Sheng et al., 2007).

There are several limitations of the study. First, the sample consists of a convenience sample of undergraduate business students. While previous research has demonstrated the value of student samples for affirming propositions about specific independent and dependent variables in specific circumstances, limitations exist pertaining to the generalizability of the results to other cohorts (Gordon, Slade, & Schmitt, 1987). Future studies using non-student samples may yield different results. Second, causal inferences cannot be drawn due to the cross-sectional survey data. Experiments could be utilized in future studies to rigorously test the proposed model. Third, the study did not investigate the role of self-efficacy in information seeking. More research is needed in examining how self-efficacy may affect the risk perceptions, affective response and information seeking intention.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Process*, *50*, 179-211.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Anderson, C., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intention. *MIS Quarterly*, *34*(3), 613-643.

CERT. (2000). CERT Advisory CA-2000-02 Malicious HTML tags embedded in client web requests. Retrieved December 5th, 2012 from http://www.cert.org/advisories/CA-2000-02.html

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Mar coulides, *Modern methods for business research* (pp. 295-336). Mahwah: Lawrence Erlbaum.

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), 386-408.

Eagly, A., & Chaiken, S. (1993). *The psychology of attitudes*. CA: Harcourt Brace.

Flinn, S., & Lumsden, J, (2005). *User perceptions of privacy and security on the web.* Presented at the Third Annual Conference on Privacy, Security and Trust (PST 2005). St Andrews, New Brunswick, Canada. Oct 12-14th.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to customer exit-voice theory. *Journal of Marketing Research*, *19*(11), 440-452.

Fornell, C., & Cha, J. (1994). Partial least squares. In R. P. Bagozzi (Ed.), *Advanced methods of marketing research* (pp. 52–78). Cambridge: Blackwell.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Friedman, B., Hurley, D., Howe, D. C., Felten, E., & Nissenbaum, H. (2002). Users' conceptions of web security: a comparative study. *Extended abstracts of CHI* (pp. 746 –747). New York, NY: ACM Press.

Furnell, S., & Karweni, T. (1999). Security implications of electronic commerce: A survey of consumers and businesses. *Internet Research*, *9*(5), 372-382.

Gefen, D., Rigdon, E. E., & Straub, D. W. (2011). Editor's comment: An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly, 35*(2), iii-xiv.

Gefen, D., Straub, D. W., & Boudreau, M-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, *4*(7), 2-75.

Geisser, S. (1975). A predictive approach to the random effect model. *Biometrika, 6*1(1), 101–107.

Griffin, R. J., Dunwoody, S., & Neuwirth, K. (1999). Proposed model of the relationship of risk information seeking and processing to the development of preventive behaviors. *Environmental Research*, *80*(2), S230-S245.

Griffin, R. J., Dunwoody, S., & Yang, Z. (2012). Testing the robustness of a risk information processing model. *Communication Yearbook, 36*, 323-362.

Griffin, R. J., Yang, J., ter Huurne, E. F. J., Boemer, F., Ortiz, S., & Dunwoody, S. (2006). *After the flood: Anger, attribution and the seeking of information.* Paper presented at the annual meeting of the Association for Education in Journalism and Mass Communication, August, San Francisco, CA.

Gordon, M. A., Slade, A. L., & Schmitt, N. (1987). Student guinea pigs: Porcine predictors and particularistic phenomena. *Academy of Management Review*, *12*(1), 160-163.

Grossman, J. (2010). *Cross-site scripting worms & viruses.* Retrieved July 6th 2011, from http://www.whitehatsec.com/home/resource/whitepapers/XSS_cross_site_scripting.html

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*, 106-125.

Huurne, E. F. J. ter (2008). *Information seeking in a risky world. The theoretical and empirical development of FRIS: A framework of risk information seeking.* Unpublished dissertation.

Huurne, E. F. J. ter, & Gutteling, J. (2005). Information needs and risk perception as predictors of risk information seeking. *Journal of Risk Research*, *25*(3), 631-650.

Johnson, B. B. (2005). Testing and expanding a model of cognitive processing of risk information. *Risk Analysis*, *25*(3), 631-650.

Johnson, E., & Tversky, A. (1983). Affect, generalization and the perception of risk. *Journal of Personality and Social Psychology*, *45*(1), 20-31.

Kahlor, L. (2007). An augmented risk information seeking model: The case of global warming. *Media Psychology*, *10*(3), 414-435.

Kahlor, L., Dunwoody, S., Griffin, R., & Neuwirth, K. (2006). Seeking and processing information about impersonal risk. *Science Communication*, *28*(2), 163-194.

Kahlor, L., Dunwoody, S., Griffin, R., Neuwirth, K., & Giese, J. (2003). Studying heuristic-systematic processing of risk communication. *Risk Analysis*, *23*(2), 355-368.

Kuttschreuter, M. (2006). Psychological determinants of reactions to food risk messages. *Risk Analysis*, *26*(4), 1045-1057.

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*, 177-187.

Lerner, J., & Kelner, D. (2000). Beyond valence: Towards a model of emotion-specific influences on judgment and choice. *Cognition and Emotion*, *14*(4), 473-493.

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), 394-413.

Loewenstein, G., Weber, E., Hsee, C., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, *127*(2), 267-286.

Lopes, A. B., & Galletta, D. F. (2006). Consumer perceptions and willingness to pay for intrinsically motivated online content. *Journal of Management Information Systems*, *23*(2), 203-231.

Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Provos, N., Rajab, M., & Mavrommatis, P. (2009). Cybercrime 2.0: When the cloud turns dark. *Communications of the ACM*, *53*(4), 43-47.

Ringle, C., Wende, S., & Will, A. (2005). *SmartPLS* (Release 2.0 (beta)). Hamburg, Germany: University of Hamburg.

Sheng, S., Magnien, B., Kumaragurum, P, Acquisti, A., Cranor L. F., Hong, J., & Nunge, E. (2007). Anti-phishing Phil, the design and evaluation of a game that teaches people not to fall for phishing. *Proceedings of the 3rd Symposium on Usable Privacy and Security,* July 18-20, 88-99.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1986). Facts versus fears: Understanding perceived risks. In D. Kahneman, P. Slovic, & A. Tversky (Eds.), *Judgment under uncertainty: Heuristics and biases* (pp. 463-489). New York, New York: Cambridge University Press.

Stern, P., & Fineberg, H. (1996). *Understanding risk: Informing decisions in a democratic society*. Washington, D.C. The National Academies Press.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society, 36*(2), 111–133.

Sutton, S. (1982). Fear-arousing communications: A critical examination of theory and research. In J. R. Eiser (Ed.), *Social psychology and behavioral medicine* (pp. 303-337). London: Wiley.

Tenenhaus, M., Esposito Vinzi, V., Chatelin, Y-M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis, 48*(1), 159–205.

Waldow, T., & Gorelik, V. (2009). Security in the browser. *Communications of the ACM*, *52*(5), 40-45.

Wang, J., & Wallendorf, M. (2006). Materialism, status signaling and product satisfaction. *Journal of the Academy of Marketing Science*, *34*(4), 494-506.

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative effect: The PANAS scales. *Journal of Personality and Social Psychology*, *54*(6), 1063-1070.

Weirich, D., & Sasse, M. (2001). Pretty good persuasion: A first step towards effective password security in the real world. *Proceedings of 2001 Workshops on New Security Paradigms*, (pp. 137-143), Cloudcroft, New Mexico.

Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly, 33* (1), 177-195.

Whitehat Security. (2011). *WhiteHat website security statistic report.* Retrieved August 3rd 2011, from http://www.whitehatsec.com/home/resource/stats.html

Witte, K. (1992). Putting the fear back in fear appeals: The extended parallel process model. *Communication Monographs, 59*, 329-349.

Yang, Z. J., McComas, K., Gay, G., Leonard, J. P., Dannenberg, A. J., & Dillon, H. (2010). From information processing to behavioral intentions: Exploring cancer patients' motivations for clinical trial enrollment. *Patient Education and Counseling*, *79*, 231-238.

Zhang, L., & McDowell, W. (2009). Am I really at risk? Determinants of online users' intention to use strong passwords. *Journal of Internet Commerce*, *8*(3-4), 180-187.

Appendix: Descriptive Statistics

Factor	Mean	STD	Source
Negative affect: when I read articles like this, I feel _____ *(scale was recoded and inverted: +2 → 1 to -2 → 5)*			Huurne (2008)
Anxious(-2) -- Comfortable (+2)	3.06	0.97	
Tense (-2) -- Content (+2)	3.13	1.06	
Angry (-2) -- Calm(+2)	3.27	1.11	
Worried (-2) -- At ease (+2)	3.19	0.94	
Afraid (-2) -- Bold (+2)	2.90	1.11	
Informational Subjective Norm (5=Strongly agree , 1=Strongly disagree)			Kahlor (2007)
The people I spent most of my time with are likely to seek information related to XSS.	2.82	0.96	
I am expected to be knowledgeable about this topic.	3.07	1.04	
Seeking information about XSS is likely to give me something to talk about with others.	3.12	1.05	
Most people who are important to me think I should stay on top of information about the topic.	2.56	1.05	
Perceived Vulnerability (5=Strongly agree , 1=Strongly disagree)			Ng et al. (2009)
I am likely to visit a website infected by XSS.	3.15	0.97	
There is a good possibility that I will be a victim of XSS.	3.21	1.10	
The chances of me being a victim of XSS are high.	3.13	0.98	
Perceived Information Gathering Capacity (5=Strongly agree , 1=Strongly disagree)			Johnson (2005)
If I wanted to, I could easily get all the information I need about XSS.	3.43	0.97	

Factor	Mean	STD	Source
I would know where to go for more information.	2.37	0.86	
I would know what questions to ask of the experts about XSS.	3.17	1.00	
Perceived Severity (5=Strongly agree , 1=Strongly disagree)			Ng et al. (2009)
Losing my sensitive information as a result of visiting an XSS infected website is a serious problem for me.	3.19	1.14	
Being directed to a fraudulent website due to XSS is a serious problem for me.	3.67	1.25	
If I lose my sensitive information, my daily life could be negatively impacted.	4.01	0.92	
Current Knowledge			Johnson (2005)
Rate your current knowledge about XSS on a scale of 0 to 100 where zero means knowing nothing and 100 means knowing everything you could possibly know about this topic.	33.10	24.96	
Information insufficiency			
Think of that same scale again. This time we would like you to estimate how much knowledge you would need to achieve a comfortable understanding of XSS. You might feel you need the same, more, or possibly even less information about the topic. Using a scale of zero to 100, how much information would be sufficient for you?	69.20	19.29	
Web risk information seeking intention (5=Strongly agree , 1=Strongly disagree)			Kahlor (2007)
I plan to seek more information about XSS in the future.	3.37	0.97	
I intend to find out more about XSS.	3.36	0.95	
In the future, I will try to seek as much information as I can about XSS.	3.25	0.93	

Biographies

Lixuan Zhang is an Associate Professor in the Hull College of Business at Georgia Regents University. She received a Ph.D. in Management Information Systems from the University of North Texas. Her major research interest includes social media, security and privacy. Her research papers appeared in journals including *International Journal of Electronic Commerce*, *Cornell Hospitality Quarterly, CyberPsychology, Behavior and Social Networking* among others.

Robert Pavur is a professor of Decision Sciences at the University of North Texas. He received his Ph.D. in Statistics from Texas Tech University. His major research interest includes applying statistical methodology to business research. He has published in such journals as the *Annals of Operations Research, IEEE Transactions on Reliability, European Journal of Operational Research, Journal of the Operational Research Society, American Statistician*, *and the Canadian Journal of Statistics.* He is a co-author of the textbook *Introduction to Business Statistics: A Computer Integrated, Data Analysis Approach* published by Cengage.

Paul T. York is an Assistant Professor of Management Information Systems in the Hull College of Business at Georgia Regents University. He received his Ph.D. in MIS from the Terry College of Business at the University of Georgia in 2011. His research interests include Social Media, Green IS, and Persuasive Technologies, and he has contributed articles to multiple top journals and national conferences. Dr. York also gained well over 10 years of IS consulting experience prior to entering academia.

Clinton Amos is an assistant professor at Weber State University. He received his Ph.D. in Marketing from the University of North Texas. His research has been published or is forthcoming in the *Journal of Advertising*, *Journal of Business Research, International Journal of Advertising*, *Journal of Marketing Communications*, *Journal of Consumer Behaviour*, *CyberPsychology & Behavior,* and the *European Journal of Marketing*