How Secure Are You? Consumer Perceptions of Cybersecurity

Sanjukta Pookulangara, Shannon Koonsman, Nicole Corts, University of North Texas, USA

Keywords: Cybersecurity, Online, Consumer, Behavior

U.S. online sales totaled $194.3 billion in 2011, up 16.1% from $167.3 billion in 2010, and accounted for 8.6% of total retail sales during the year, up from 7.6% in 2010 (Enright, 2012). Although e-commerce has become popular, internet privacy violations and cyber attacks to the e-commerce systems are also on the rise with violations such as failing to protect sensitive customer and employee data, which have put these individuals at high risk of being victims of personal-identity and credit-card thefts (Farrell, Sheer, & Garrison, 2009). In fact, industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion (Harrison, 2011). Thus it can be stated with a high degree of conviction that cybersecurity is detrimental both to the business as well as the consumer and needs to be investigated

Rationale of the Study: There is a distinct difference between cybersecurity and privacy. Privacy can be described as a two-dimensional construct, involving physical space and information (Goodwin 1991). On the other hand cybersecurity can be defined as ‘‘a security relevant system event in which the system's security policy is disobeyed or otherwise breached’’ (Shirey, 2000). In other words, cybersecurity deals with damage to, unauthorized use of or exploitation of electronic information and communications systems that ensure confidentiality, integrity and availability.

Given the importance of impact on cybersecurity, there is a distinct lack of research which examines this important phenomenon from the consumers' perspective. There have been studies that have examined privacy online in various contexts including value, perceived risk, trust, service quality, cross-cultural comparison (Zeithaml, Parasuraman, Malhotra, 2002; Wolfinbarger & Gilly, 2003); however, none of the studies have investigated cybersecurity. In most of the studies, privacy and security concerns are treated as a single construct with security examined as one of the dimensions of the overarching privacy concerns (Liu, Marchewka, Lu, & Yu, 2004; Xu & Teo 2004). Thus, this study is a step toward filling the gap in the literature especially and was exploratory in nature and analyzed consumers' perception of cybersecurity using focus group interviews.

Results: Data for personal interviews was collected via convenience sample resulting in ten focus groups (n=53). The questions for the in-depth interviews were based on the existing literature (e.g., eCommerce Trust Study, 1999; Wang, & Emurian, 2005) and consisted of open-ended questions to elicit candid responses from participants. After analysis of the interviews, the following themes emerged:

(1) *Defining Cybersecurity:* The focus group participants were asked to define the concept of cybersecurity. Most of the participants indicated that it had a relationship to the Internet with definitions such as “staying secure online”; “preventing identity fraud online”; and “protecting private information”.

(2) *User-Generated-Content (UGC)* (e.g., reviews of products, links to social networking sites such as Facebook, Twitter, and Pintrest): The participants were vocal and unanimous that the inclusion of UGC such as reviews and links to Facebook pages increased the credibility of the website.

(3) *Informational Attributes:* The participants indicated that they paid attention to the kind and amount of information requested either while browsing a website or prior to the

completion of the purchase transaction and it directly influenced their perception of the website in terms of secure or insecure.

(4) *Retailer Channel Attributes*: The channels of operations and nature of the retailer (e.g. pure-play vs. multi-channel) influenced security perceptions for all the participants. Channel synergies were important to the participants and contributed to the perception of security online.

Conclusions and Implications: Both e-tailers and researchers understand the importance of cybesecurity to the growth of their businesses, and the necessity of taking proper measures to ensure that security threats are eliminated or significantly reduced so that consumer confidence in the Internet as an alternative means of shopping is maintained (Smith, 2004). However, as this study indicates, the role of consumer behavior and perception of cybersecurity is equally critical to the success of e-tailers. Online shopping phenomena are governed by a number of consumer acceptance and behavior characteristics, and this study provides highlights important variables that influence consumers' confidence while shopping online. Overall, e-tailers need to increase not only their cybersecurity measures, but also their consumers' perception of a high standard of security in order for the success of both individual e-tailers and the future of e-commerce itself.

References

eCommerce Trust Study. (1999). *Cheskin Research And Studio Archetype/Sapient*. Retrieved on March 11, 2013 from: http://www.added-value.com/source/wp-content/uploads/2012/01/17__report-eComm-Trust1999.pdf

Enright, A. (2012). E-commerce sales jump 16% in 2011: The U.S. Commerce Department says consumers spent $194 billion online in 2011.*Internet Retailer*. Retrieved on February 20, 2012 from http://www.internetretailer.com/2012/02/16/e-commerce-sales-jump-16-2011

Farrell, C. B., Sheer, A.,& Garrison, L. (2009). *CVS Caremark settles FTC charges: Failed to protect medial and financial privacy of customers and employees* [Press release]. Retrieved on February 20, 2012 from http://www.ftc.gov/opa/2009/02/cvs.shtm

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing, 10*(1), 149-66.

Harrison, E. (2011). Obama administration outlines cybersecurity plan. *Strategic Initiatives*. Retrieved on February 20, 2012 from http://www.techzone360.com/topics/techzone/articles/174153-obama-administration-outlines-cybersecurity-plan.htm

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2004). Beyond concern: a privacy–trust–behavioral intention model of electronic commerce. *Information & Management*, *42*(1), 127-142.

Shirey, R. (2000). Internet security glossary. *The Internet Society*. Retrieved on February 19, 2012 from

Wolfinbarger, M. & Gilly, M.C. (2003). eTailQ: Dimensionalizing, measuring and predicting retail quality. *Journal of Retailing, 79*(3), 183–198.

Xu, H., & Teo, H. H. (2004, December). Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective. In *Proceedings of the Twenty-Fifth International Conference on Information Systems* (pp. 793-806).

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105-125.

Zeithaml, V. A., Parasuraman, A., & Malhotra, A. (2002). Service quality delivery through web sites: A critical review of extant knowledge. *Journal of the Academy of Marketing Science, 30*(4), 362-375.