Cybersecurity:
What Matters to Consumers – An Exploratory Study

Sanjukta Pookulangara
University of North Texas, USA

INTRODUCTION

Cybersecurity is now a persistent business risk and it's a trend that will likely continue. (Global State Of Security, 2015)

U.S. online sales is expected to grow from $263 billion in 2013 to $414 billion in 2018, a compound annual growth rate of 9.5% (Enright, 2014). Although e-commerce has become popular, Internet privacy violations and cyber attacks to the e-commerce systems are also on the rise. Cyber-attacks have impaired or even shut down the e-commerce activities completely by damages such as website defacement, denial of service, price manipulation, financial fraud, or data breach (Hovanesian, 2008). Global State of Information Security (2015) a survey conducted by PricewaterhouseCoopers has indicated that the total number of security incidents has increased 48% over 2013. In fact industry estimates of losses from intellectual property to data theft in 2013, range as high as $1 trillion (Ackerman, 2013). Furthermore, a study by Ponemon Institute indicated that the average cost of cybercrime for U.S. retail stores more than doubled from 2013 to an annual average of $8.6 million per company in 2014 (Ponemon Institute, 2014). 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.

The Internet is complex in nature. The governments and businesses worldwide have been tasked with providing secure e-commerce trade practices, and laws to enforce those practices. In the early 2000's, the United States established CERT (Computer Emergency Readiness Team), which is the operational arm of the National Cyber Security Division at the Department of Homeland Security (DHS); the mission being "to improve the nation's cyber security posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans" (US-CERT, 2012). Currently, DHS works directly with public and private partners to enhance cybersecurity (Combat Cyber Crime, 2014). On top of this measure of security, there are countless individual software programs that companies and individuals alike use to combat cybercrime (e.g., Norton, MacAfee and other anti-spam, anti-spy and firewall software). Although these programs are utilized to secure all major online websites, more than half of consumers are either unsure or not confident at all in the security of their personal information when shopping both in-store and online which is ultimately hindering the development of e-commerce to its full potential.

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, and service quality (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 (Xu & Teo 2004). Some of the researchers

DOI: 10.4018/978-1-4666-9787-4.ch012

have conceptualized that privacy is dependent upon information security (Chellappa, & Pavlou, 2002). On the other hand, according to Belanger, Hiller, & Smith (2002), privacy and security concerns should be conceptualized as distinct, and there is a lack of understanding of their relations (see also Chang, Cheung, & Lai, 2005; Vijayasarathy 2004).

There is a distinct difference between cybersecurity and privacy, with privacy being described as a two-dimensional construct, involving physical space and information (Goodwin, 1991). The Internet security glossary [RFC 2828] delineates security from privacy as an event where ''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, exploitation of electronic information and communications systems that ensure confidentiality, integrity and availability. Thus, the proposed study is a step towards filling the gap in the literature especially given the high importance of cybersecurity and its impact on the society. The study was exploratory in nature and analyzed consumers' perception of cybersecurity using focus group interviews.

RELATED LITERATURE

Defining Cybersecurity

According to Kalakota and Whinston (1996), security threat has been defined as a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse." This study adopts the definition of cybersecurity from Dunn (2005), who conducted a comparative analysis of cybersecurity initiatives on a worldwide scale. Thus, cybersecurity can be defined as: (1) actions and measures, both technical and non-technical, with the express purpose of protecting computers, networks, software, data and other related digital technologies from all threats, (2) the degree of protection resulting from the adoption of these activities and measures, and (3) the professional activity of implementing the above mentioned actions and measures including research, analysis and policy development (Dunn, 2005).

The importance of cybersecurity cannot be undermined, as evidence suggests that the principal reasons why people do not purchase via the Internet are related to online security and policy, and reliabilities of companies (Gefen, 2000). It is imperative that cybersecurity measures are developed to ensure the safety of consumer privacy and information in order to allow for a carefree shopping experience, without which e-commerce could not be sustained (Smith, 2004; Gradon, 2013). Consumers view the Internet purchasing as a conduit for private data interchange, an activity which entails primary interactions with the Internet and World Wide Web and the extent to which consumers trust this computerized medium affects their overall Internet purchasing behavior (McCole, Ramsey, & Williams, 2010). Thus, in general, neither consumers, nor retailers, know enough about what threats are most important on the Internet and how they can be detected and countered (Lesk, 2011).

Antecedent of Cybersecurity: Website Characteristics

Cybersecurity, may be defined as the subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations (Flavián, & Guinalíu, 2006). The actual attributes of the e-commerce site play a large role in the consumers' de-