Decision Support Systems 83 (2016) 47–56

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults

Rajarshi Chakraborty [a], Jaeung Lee [a], Sharmistha Bagchi-Sen [b], Shambhu Upadhyaya [c], H. Raghav Rao [d,*]

[a] Department of Management Science and Systems, State University of New York at Buffalo, Buffalo, NY, USA
[b] Department of Geography, State University of New York at Buffalo, Buffalo, NY, USA
[c] Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY, USA
[d] Department of Information Systems and Cybersecurity, University of Texas at San Antonio, San Antonio, TX, USA

ARTICLE INFO

Article history:
Received 24 November 2014
Received in revised form 8 November 2015
Accepted 25 December 2015
Available online 16 January 2016

Keywords:
Online shopping
Data breach
Trust
Perceived risk
Internal monitoring
Age

ABSTRACT

Data breaches through hacking incidents have become a significant phenomenon in the world of online shopping. These breaches can result in loss of personal data belonging to customers. This study builds a research model to examine people's intention to engage in e-commerce in the context of a significant data breach (the Target breach in December 2013). In addition, this paper focuses on the difference in responses regarding post-breach online shopping intent among younger adults (below 55 years) and older adults (senior citizens—above 55 years). Our findings show the importance of internal (self) monitoring of bank transactions in reducing the effect of perceptions of severity of data breaches on post-breach online shopping intent particularly for senior citizens. The study also demonstrates that perceptions of severity of a hacking incident are significant drivers of perceived online shopping risk for both age groups. Further, perceptions of severity of a hacking incident are significant drivers of post-breach online shopping intent but only marginally significant for younger adults. Trusting beliefs in online shopping services and attitude toward e-commerce are significant for the older generation for post-breach online shopping intentions and also for younger adults. Gender is significant for seniors while it is not significant for younger adults. The impact of perceived online shopping risk on post-breach online shopping is significantly different between the two age groups. The implication of this research lies in informing shopping websites the need to prepare better plans for notifying customers about not only data breaches but also their proposed mitigation steps so as to increase trust and reduce perceived risks associated with online shopping.

1. Introduction

Online shopping has been steadily gaining acceptance around the world, especially in the United States [19]. Online shopping websites have in some instances replaced physical stores (e.g., books and electronics) [53]. The rise in online shopping has partially been attributed to the success of secure payment methods through credit and debit cards. According to recent findings [60], these cards account for over 70% of payment methods used for online shopping. In addition to the increasing payment convenience, time-saving has also been a key factor in the adoption of e-commerce [3]. Online stores have improved the overall shopping experience by mimicking the amenities of a physical shopping experience in a virtual world [69]. One such example would be saving items in a "shopping cart" and checking out at a later point. This workflow is akin to dropping objects in a physical shopping cart and walking around the store until it is time to check out. This convenience in online shopping experience has reduced the perceived risks towards online shopping that could have been attributed to the lack of physical tangibility [54]. While Amazon has been largely at the forefront, several traditional retail chains are now active online. Target, Walmart, and Best Buy often experience as much traffic and transactions through their websites as they do through their physical stores [5].

The literature on information systems and marketing is rich with studies about the adoption and success of online shopping [12,39,52,66]. Most of these studies have examined trust, convenience, and privacy as antecedents. Trust and privacy concerns, in particular, have remained of sustained interest given the ever-evolving risks and attacks associated with online shopping over the years. According to statistics released by the Identity Theft Resource Center [25], in the first half of 2014, 381 reported data breaches led to the exposure of over 10 million records of individuals in the United States. This presents significant danger to personal and sensitive data stored in millions of websites. The most danger is faced by websites that allow customers to make transactions. These include shopping websites where hackers are still able to get past sophisticated firewalls and other security software as was the

* Corresponding author. Tel.: +1 210 458 6300; fax: +1 210 458 6305.
E-mail addresses: rc53@buffalo.edu (R. Chakraborty), jaeungle@buffalo.edu (J. Lee), geosbs@buffalo.edu (S. Bagchi-Sen), shambhu@buffalo.edu (S. Upadhyaya), mgmtrao@gmail.com (H. Raghav Rao).

http://dx.doi.org/10.1016/j.dss.2015.12.007
0167-9236/

case with Target in 2013 [68]. In addition to the technical challenges, often personnel in charge of the security of these websites fail to take pro-active actions. Customer names, addresses, email addresses, account numbers, and transaction information are often exposed as a result of many of these breaches [18].

Given that online shopping is an integral part of today's economy, it is important to examine how people's attitude towards it is affected by threats to their personal information. In this paper, we have specified the study's context as the Target data breach [68]. We evaluate the effect of traditionally held notions of trust, security risk, and behavior in online shopping [50]. This paper's contribution is threefold. First, we have incorporated people's internal monitoring to scrutinize artifacts that might be affected by data or other security breaches. We posit that monitoring habits mitigate some of the security concerns and placate fears that may arise in the aftermath of security incidents like the Target and Neiman Marcus data breaches. Second, while purchasing intent has been studied in the field of information systems, it has not been explored in the aftermath of a major data breach incident that is likely to alter intent. Third, the perspective of generational differences has not been examined in prior literature. This paper looks at the difference between two age-based demographics—one below 55 and the other above 55 years. Traditionally, the latter is referred to as the "senior citizens" generation (older generation) with those between 55 and 60 years representing the first tail of it. The reason for this comparative approach is twofold: (1) research has shown significant differences in privacy concerns between older and younger computer users [27] and (2) testing our hypotheses on a younger sample gives us perspective to interpret the findings from the older population. As our findings will show later in this article, there are significant differences in certain fundamental causality aspects of trust and risk-driven behavior on the Internet between these two broad categories of the U.S. population.

To summarize, this paper focuses on the difference in responses regarding post-breach online shopping intent among younger adults (below 55 years) and older adults (senior citizens—above 55 years). Findings show the importance of internal (self) monitoring of bank transactions in reducing the effect of perceptions of severity of data breaches on post-breach online shopping intent, particularly for senior citizens. The study also demonstrates that perceptions of severity of a hacking incident are significant drivers of perceived online shopping risk for both age groups, and while they are significant drivers of post-breach online shopping intent for seniors, they are only marginally significant for younger adults. Trusting beliefs in online shopping services and attitude towards e-commerce are significant for the older generation for post-breach online shopping intentions and also for younger adults. Gender and the impact of perceived online shopping risk on post-breach online shopping are significantly different between the two age groups.

In the remainder of this paper, we first discuss recent data breaches serving as the background of our study. Then we present the development of our research model. After that, the data collection and the analysis are discussed, following which the paper concludes with a focus on the current limitations and the opportunities for future research.

2. Prior literature

According to a report by the Identity Theft Resource Center (ITRC) Dark_Reading [21], 73% (365 respondents out of 500 respondents) answered that they may not purchase merchandise from online websites that have experienced security breaches. Such incidents have triggered customers' protective behaviors such as avoiding using online stores, switching to another online store, and using offline stores [41]. Khalifa and Limayem [37] also found that customers will shop on e-commerce sites more frequently if they do not worry about risks of security breaches.

In addition to online shopping cases, offline business research has also provided similar findings. Belanger et al. [7] studied the impact of security breaches on hotel revisit intention, likelihood of hotel recommendation and satisfaction. Their results showed that breaches resulted in negative impacts on all outcome variables. This indicates that consumers are highly concerned about data breaches.

Customers' credit card information and other personal information are some of the most commonly stolen items during data breaches into the systems of shopping websites [57,73]. Upon a breach and an improper access to such information, these customers become vulnerable to unapproved purchases. Information like mailing address also has the potential of being misused for exploits. Often, such exploits can be harder to detect and their effects can be felt by victims in the real world. Online transactions are seldom carried out with complete information about privacy protection from the store owner [1]. On the other hand, customers of online shopping are rarely given the option to choose what information they should provide to the website for the transaction and any additional benefits. For example, storing information about one's favorite local store requires providing one's zip code. Often, a transient piece of information for the completion of a transaction may be enough to put a customer at risk after a data breach. Thus, any data breach into these businesses can potentially lead to identity theft.

Baier [4] defined trust as the "accepted vulnerability to another's possible but not expected ill will toward one" (p. 99). Customers know the kind of risk they are taking; however, the individual customer is often disposed to trust that nothing bad will happen to them. They have positive expectations regarding online shopping websites in their provisioning of shopping services. A fundamental antecedent of technology adoption [22] is the decision to trust a technological artifact. Trusting or distrusting of an artifact is based on an individual's general disposition to trust others [47]. The Web Trust Model (McKnight et al. [47] explains the causality of trust on behaviors in the form of decisions made on the Internet. These decisions usually pertain to actions like shopping and sharing information on the Internet. More recently, however, researchers have started to investigate these decisions in the light of both negative and positive beliefs about the potential outcomes [45]. While most people may trust their frequently visited shopping websites with respect to service quality, repeated stories of breaches may arouse concerns and distrust among them. Media reports about breaches can lead to a significant drop in consumers' trust in the security-related capabilities of shopping websites. Whether trust and distrust are distinct constructs or the opposites of a trust–distrust continuum has been debated. Omodei and McLennan [56] proposed that trust and distrust are two ends of the same scale. Luhmann [43] posited that while trust and distrust are essentially the same construct, they are distinct functional equivalents. Therefore, in our paper, we considered trust and distrust (as a lack of trust) in the same construct.

Disposition to trust has been constantly changing through generations [38,51,67]. For instance, around 1996, Internet through the Web (i.e. the Mosaic Web browser) became mainstream. People at that time who were in their late 30s (i.e. 55 and above at the present time) were the last generation to whom Internet was introduced as a niche technology. Studies about differing perceived usefulness of IT across age groups have shown that the general perception about the Internet is different among people above 55 and those below [49]. According to [64], younger Americans are less trusting of fellow human beings than their older counterparts. [59] have shown that there is no significant difference between younger baby-boomers and older baby-boomers in terms of most behavioral variables. Also, traditionally, the age of 55 years has been shown to be an important lower bound for studying Internet behavior in the older population [70]. The fundamental concepts of trust and risk-taking are the differentiators between younger adults and people over 55. In the context of online shopping, given the importance of security and privacy, awareness about security hazards can also be a significant differentiator. Grimes et al. [30] have shown that older adults are generally less aware of security hazards on the Internet compared to their younger counterparts. Also, older adults tend to be generally more risk-avoiding than younger adults,