Decision Support Systems 71 (2015) 62–77

Contents lists available at ScienceDirect

Decision Support Systems

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

Trust violation and repair: The information privacy perspective

Gaurav Bansal [a,*], Fatemeh Mariam Zahedi [b,1]

[a] Austin E. Cofrin School of Business, University of Wisconsin - Green Bay, 2420 Nicolet Dr, Green Bay, WI 54311, United States
[b] Sheldon B. Lubar School of Business, University of Wisconsin - Milwaukee, 3202 N. Maryland Ave., Milwaukee, WI 53211, United States

ARTICLE INFO

Article history:
Received 2 January 2014
Received in revised form 6 December 2014
Accepted 24 January 2015
Available online 31 January 2015

Keywords:
Trust violation
Trust repair
Privacy concern
Hacking
Unauthorized sharing

ABSTRACT

With the pervasive use of the Internet, customer information privacy violation is on the rise and companies could suffer by losing their customers' trust. While previous literature has identified factors that influence trust, less attention has been paid to how trust may be rebuilt after it is violated by negative events regarding customer information privacy. The study synthesized two salient theories (the attribution theory and the organizational justice theory) to investigate the process by which trust is violated by privacy breaches and the extent of its repair by company responses. We examine the moderating effects of two types of privacy violation—hacking and unauthorized sharing—on the trust violation and repair process. We investigate the efficacy of three response types—apology, denial and no response. Data were gathered using a controlled, scenario-based lab experiment. Our results showed the significant moderating impact of violation type on the process of trust violation and repair. Apology emerged as a universally effective response, although its reparative power was far less in unauthorized sharing than in hacking. Denial emerged as a complex response. Furthermore, the results showed that trustworthiness beliefs (ability, integrity, and benevolence) are differently impacted in the violation–repair process. Details of theoretical and managerial implications are discussed.

1. Introduction

The frequency and extent of privacy violation in cyber space has increased in scope and intensity and exposure of customer private data on a large scale has become a common occurrence. For example, in May 2013, private data of 50 million customers of LivingSocial, the second largest daily-deal company behind Groupon were hacked [5]. A report by Internet Crime Complaint Center (IC3) shows that individual victims have lost an average of $4600 in 2012 [23]. In a survey of 583 companies, 90% reported that they have been hacked at least once in 2011 and 50% had little confidence that they could prevent being hacked again [76]. Although there are strong laws for privacy protection, the ease of collection and transfer of customer private data and an increasingly large appetite to combine and integrate customer data for market analysis has made the unauthorized use of customers' private data tempting for companies in their pursuit of larger market share and higher profits [46]. While hacking is an external and unpredicted event, unauthorized use of customers' private data is an internal decision by companies. However, both being breached by hackers and intentional unauthorized use of customers' private data could have damaging consequences for companies, as was demonstrated by the reaction of Facebook users to its change of privacy policy and its more obtrusive search method exposing customer information on Facebook [63].

Breach of customers' private information could violate their trust in the company. It is widely acknowledged that trust is necessary in order for any business to thrive, and it is even more necessary in online environments where the trustor may feel more vulnerable when dealing with a faceless and remote trustee. Loss of trust leads to lost sales and other irreparable and "devastating damages" [72: p. 85]. The consequence of the violation is that it erodes subsequent user trust which may reduce the extent to which the trustor (user) will cooperate with the trustee [41]. Trustor in this research is the user who interacts with the website and develops trust in the business practices of the trustee. Trustee is the business entity or the company that owns the website. Following the extant literature on trust, we define trust as a psychological state of willingness to accept vulnerability based upon positive expectations of the intentions or behavior of the trustee in matters important to the trustor [37,45,57]. It has been reported that negative events and transgressions reduce trust [73]. Bies and Tripp [8] define trust violation as "unmet expectations concerning another's behavior or when [the trustee] does not act consistent with one's values" (p. 248). We, define violated trust as the level of trust after a negative salient event or transgression that could be ascribed to the trustee [72]. Repaired trust is defined as the level of trust after the trustee has taken positive actions to repair the trust following a violation, which restores trustor's willingness to be vulnerable to the trustee's future actions [24,72].

* Corresponding author. Tel.: +1 920 465 2216; fax: +1 920 465 2660.
E-mail addresses: bansalg@uwgb.edu (G. Bansal), zahedi@uwm.edu (F.M. Zahedi).
[1] Tel.: +1 414 229 6454; fax: +1 414 229 6957.

http://dx.doi.org/10.1016/j.dss.2015.01.009
0167-9236/

In other words, in the sequence of pre-violation (prior) trust, post-violation trust, and post repair trust, two events take place: negative information about the event is ascribed to the trustee and a trustee's social-account response (e.g., a public apology) intended to mitigate the negative consequences of the event and restore trust. Following Sitkin and Bies [64] and Tomlinson and Mayer [72], we define a social account as a public explanation of a violation event. While previous literature has investigated the factors that influence trust, less attention has been paid to how trust may be restored after it is violated. Several researchers [36] have recently called for a deeper analysis of trust repair processes. The study of trust repair has recently started to gain momentum in Management [22,36,59,72], Marketing [77] and MIS [29,41]. However, there is inadequate research in trust repair, particularly after breach of customers' information privacy. There is a need to examine trust violation and repair in online environments from an information perspective, since information serves as the key resource for any online business in general and e-commerce in particular. Moreover, any trust rebuilding examination should be preceded by an examination of violated trust. Echoing similar sentiments Schoorman et al. [59] stated that "it is critical to first understand how it [trust] was damaged in the first place, since different means of damaging trust are likely to require different repairing responses" (p. 349).

Hence the research questions in this study are: (1) what is the process of trust violation and repair when an information privacy violation occurs? (2) What are the reparative impacts of social accounts? (3) What is the moderating role of violation type in the trust violation and repair process?

To answer these research questions, we synthesize the attribution theory [78] and the organizational justice theory [15] to develop a conceptual model for the process of trust violation and repair when customers' private information has been violated. Based on the taxonomy of the attribution theory, we consider two types of privacy violation: hacking and unauthorized sharing of customers' private information. Moreover, we investigate how violated trust could be repaired by responding via a social account—apology, denial and no response. More importantly we examine the moderating influence of violation type on the trust violation and repair process. The research methodology in this work is a scenario-based controlled experiment. The results provide significant theoretical and managerial implications.

The paper is organized as follows. The next two sections present theoretical justifications and a salient review of the literature. The research model and the hypotheses are reviewed next, followed by research methodology, analysis and results. Contributions and implications are then discussed. The last section presents conclusions, limitations and future research opportunities.

2. Review of salient theories

There are two theories that are salient in trust violation and repair: attribution theory [78,79] and organizational justice theory, which has emerged from social exchange theory and justice literature [15]. Both theories have their genesis in social psychology and human motivation. They have migrated to the management literature with focus on outcomes, performances and their causes, and have been applied in studying trust violation and repair [36,38,61,72]. However, the two theories diverge in the specificity of their causal antecedents and the scope of their goals.

2.1. Attribution theory

The goal of the attribution theory is to identify the causes that can be attributed to performance outcome [30]. However, it was Weiner's seminal work (1985) that proposed the attribution theory and a general taxonomy for causal attributions. The attribution chain starts when a person encounters "a *subjectively* [emphasis added] important act" [78: p. 564] which sets "the boy [person] overtly or covertly wondering" (p. 564). Individuals who encounter negative outcomes feel emotional displeasure that leads them to seek causes [72,78]. The causal attribution has three primary, independent, and continuous dimensions: locus of control (e.g., internal to the trustee vs. external to the trustee), controllability (e.g., the extent of "volitional control" by the trustee or another actor), and stability ("the degree to which the cause is perceived to either fluctuate or remain constant") [72: p. 88].

Although the use of these dimensions is based on the context and individual interpretations, the generality of the dimension remains constant [78]. For example, a student may attribute failing a test to his/her laziness (internal, controllable, and stable), illness (external, uncontrollable, and chance/unstable), or the teacher's habit of giving difficult tests (external, uncontrollable, stable). In a later discussion of the attribution theory, Weiner [79] raises the distinction between pre- and post-event perceptions, which applies well to the concepts of pre- and post-trust when the event is a violation that could impact trust.

The generalized taxonomy in the attribution theory allows for theorizing and predicting various behaviors, reactions, outcomes, and performances depending on the category of attributable cause [78,79]. For example, two negative events with different attributable causes with different loci, controllability and stability—say one internal/controllable/stable and the other external/controllable/stable—could produce two distinctly different cognitive, emotional and behavioral consequences in the actor, one accepting responsibility, regret, and taking corrective action, and the other casting blame, fueling anger, and demanding punishment and redress. This is particularly helpful in our study since we deal with two distinct types of events related to privacy violation: hacking and unauthorized sharing of customers' private information. Drawing on the taxonomy of the attribution theory, we will argue that differences in the attribution dimensions of hacking and unauthorized sharing produce different impacts on the victims.

Moreover, the attribution theory posits that outcomes of causal attribution are not permanent and could be invalidated or modified by reparative efforts such as social accounts [71,72,78], thus mitigating the negative outcomes, such as repairing trust after a violation event [71]. This is another salient aspect of the attribution theory to our study since understanding the efficacy of mitigation actions after a privacy violation is an important topic that has not been addressed in the privacy literature thus far.

2.2. Organizational justice theory

The focus of this theory is employees' perceived justice of managers' performance in terms of decision-making and employee-evaluation processes. The organizational justice theory has four categories of justice as antecedents of performance: procedural justice, distributive justice, informational justice, and interpersonal justice [11]. Procedural justice "reflects the perceived fairness of decision-making processes," and distributive justice is "the perceived fairness of the decision outcomes." Interpersonal justice is the fairness and respect in communication of outcomes, and information justice is "truthfulness and adequacy of explanations" [15: p. 200]. The violation of justice in these four dimensions leads to cognitive, emotional and behavioral consequences for the victims, such as their trust, trust beliefs, commitments to the organization, and job performance [12,13]. In a meta-analysis of 493 independent samples, Colquitt et al. [15] have produced an extensive account of the research in the organizational justice theory and have identified the differential impacts of justice dimensions on employees' trust, commitment, perceived organizational support, leader–member exchange, affect and behaviors.

The organizational justice theory is also salient to our study since informational justice is the specific antecedent relevant to protecting customers' private information. The arguments related to the impact of justice violation on trust in this theory could add rigor to our investigation of privacy violation. Thus, we synthesize the attribution theory and the organizational justice theory in conceptualizing the process of