Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2018 Proceedings | Midwest (MWAIS)

5-2018

Timing of Data Breach Announcement and E-Commerce Trust

Steven Muzatko
University of Wisconsin–Green Bay, muzatkos@uwgb.edu

Gaurav Bansal
University of Wisconsin–Green Bay, bansalg@uwgb.edu

TIMING OF DATA BREACH ANNOUNCEMENT AND E-COMMERCE TRUST

Steven Muzatko
University of Wisconsin–Green Bay
muzatkos@uwgb.edu

Gaurav Bansal
University of Wisconsin–Green Bay
bansalg@uwgb.edu

ABSTRACT

The primary contribution of this study is the examination of whether the timeliness in announcing the discovery of a data breach impacts the reduction in consumer trust in an e-commerce company, as well as later trust rebuilding efforts taken by the company. This study examines the effect of both trust reducing events (announced data breaches) and trust enhancing events (provision of data protection) on the level of perceived trust. The timeliness of the announcement of the breach by an e-commerce company was manipulated between two randomly assigned groups of subjects by changing the announcement of the breach between immediately upon its discovery by the company's management and an announcement made two-months after the breach was discovered. The results suggest that companies that delay the announcement of a data breach are likely to suffer a larger drop in consumer trust than those companies that immediately disclose the data breach.

Keywords

Data breach, website trust, trust violation, trust repair, privacy concern.

INTRODUCTION

Trust in e-commerce plays an important role in the willingness of parties to exchange money and goods without having direct personal contact. The examination of this trust relationship is important given the volume of business transactions that occur through e-commerce websites. One aspect of e-commerce trust revolves around the privacy of consumers' personal information. Given the large numbers of consumers and companies affected by data breaches, the study of changes in trust because of a privacy breach is of contemporary importance.

There are numerous examples of situations where e-commerce companies gather and maintain private information about their customers, only to have that information disclosed to others without customer authorization. For instance, Equifax announced a data breach in September 2017 that might have compromised the personal information of 143 million of its customers (Equifax Data Breach, 2017). These types of breaches are prevalent and can be very costly. In 2017, the Identity Theft Resource Center tracked 1,579 data breaches that compromised 178,955,069 individual records (Identity Theft Resource Center, 2017). One study estimates the average total cost of a data breach is $3.62 million, and the average cost of each record lost or stolen is $141 (Ponemon Institute, 2017). Other empirical studies provide evidence of adverse stock market declines for companies that disclose data breaches (Malhotra and Malhotra, 2011; Martin, Borah, and Palmatier, 2017; Myung, Osei-Bryson, and Dorantes, 2009; Schatz and Bashroush, 2016).

Companies have a legal obligation to disclose data breaches. Forty-eight states have enacted some legislation requiring companies to notify individuals affected by a data breach. However, the

requirements related to timing or method of the notice varies from state to state (National Conference of State Legislatures, 2018). Under certain circumstances, companies have the discretion to withhold publicly announcing a data breach for some time after discovering that customer data was compromised.

The timing of the announcement is an important decision made by companies that suffer a data breach (Jaeger, 2012). Equifax, referred to earlier, was heavily criticized because it waited approximately five weeks after it discovered the data breach to make a public announcement. The delay in announcing the breach brought Equifax under scrutiny of the United States Congress and the fallout over failing to announce the breach may have led to the company's chief executive officer being fired (Lieber and Cowley, 2017). Companies must weigh the cost of potentially having to revise information if they disclose a breach immediately against the additional loss of confidence by customers who review the delay in reporting negatively.

LITERATURE REVIEW AND RESEARCH MODEL

Bansal and Zahedi (2015) examine privacy-based trust violation and repair through the lens of attribution theory (Weiner 1985) and organizational justice theory (Colquitt, Conlon, Wesson, Christopher, and Ng, 2001). They conclude that attribution theory supports changes in trust due to events such as privacy violations and trust restoring events.

McAllister (1995) examined trust among managers and professionals in organizations. Drawing on sociological and social-psychological literature on trust, McAllister proposed a theoretical model where trust is multi-dimensional, comprised of both competence and affective components. Competence-based trust is developed through reliability and dependability, whereas affect-based trust is a result of actions that affect emotions such as expressing care or concern for another party.

Several studies have demonstrated that data breaches lead to reduced consumer trust in companies that announce a data breach. Liao, Luo, and Gurung (2009) develop a model of rebuilding trust after a trust violation in an electronic business to consumer (B2C) setting; they also provide empirical survey data that confirms the effectiveness of trust rebuilding activities in trust restoration. Bansal and Zahedi (2015) also examined the difference in trust repair given the type of action taken by a company—apology, denial, and no response. They find that apology is the most effective response to rebuild trust after a trust violation.

The model developed in this study draws upon an agent-based model developed by Choi and Nazareth (2014). The model views the trust between a consumer and an e-commerce company as an interpersonal relationship. In this relationship, the trust between parties can be impaired and then later restored. The reduction of trust can be impacted by an e-commerce company's response to a trust violation. After a trust violation, the restorative action the company takes also plays a role in determining whether trust is restored, degraded, or broken (Choi and Nazareth, 2014).

This study extends extant research in this area by studying whether a delay in the disclosure of a data breach by the management of the e-commerce company affects violated and repaired trust.

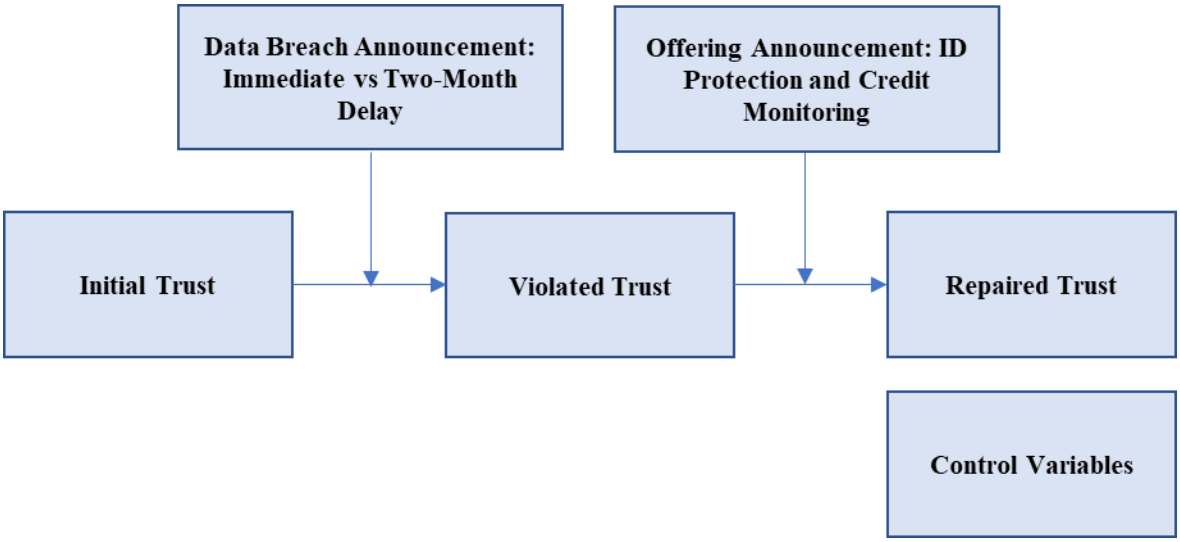

Figure 1. Research Model

HYPOTHESES

Based on McAllister's (1995) model that trust is multi-dimensional, events will elicit greater changes in trust if they are perceived to affect more than one dimension. For instance, a data breach would decrease competence-based trust as the reliability and dependability of the e-commerce company would be perceived as being impaired. If a company's management is not forthright in disclosing the breach, the e-commerce company might be considered to lack care or concern for customers. Thus, a company's management that delays the announcement of a data breach would decrease a second dimension of customer trust, that is affect-based trust.

Building upon the Choi and Nazareth's (2014) agent-based model and McAllister's (1995) reasoning that trust is multi-dimensional, the following hypotheses are proposed. First, a data breach can be perceived to be the absence of appropriate security controls of an e-commerce company. Customers have an expectation that the e-commerce company will maintain security measures to protect private information, and the breach implies a lack of reliability on the e-commerce company's part. A breach would reduce one dimension of trust – competence-based trust.

Therefore, a data breach leads to a reduction in trust.

H1: Violated Trust will be lower than Initial Trust.

Choi and Nazareth develop a conceptual framework for rebuilding trust after a trust violation has occurred. One reconciliation tactic that can be used by an e-commerce company to rebuild trust is restorative action. The restorative action is used to compensate for damages that result from the data breach and the compensation is a way to rebuild trust in the e-commerce company.

Therefore, offerings (such as credit monitoring) lead to an increase in trust.

H2: Repaired Trust will be larger than "Violated Trust".

A company that is not forthright in sharing information about the breach of private customer data will reduce a second dimension of trust, the customer's affect-based trust. The action of withholding the information about the breach can be perceived as management's lack of concern for customers. Thus, companies that report the news of the breach immediately upon discovery will have greater customer trust than companies that share the information with delay.

Therefore, prompt reporting of a data breach is positively associated with Violated Trust.

H3: Violated Trust is higher if a company discloses the breach immediately rather than delays reporting of breach.

One challenge of restoring trust after a trust violation is that parties that violate the trust relationship must not only reestablish initial trust but must also overcome the negative effects of the trust violation (Choi and Nazareth, 2014). Trust restoration has also been shown to more difficult in cases where the trust violation relates to matters of integrity, rather than matters of competence (Kim, Ferrin, Cooper, and Dirks, 2004). In situations where violated trust is lowered because it has been impacted on more than one dimension (i.e. both competence-based trust and affect-based trust), it will be more difficult to repair trust.

Therefore, prompt reporting of a data breach is positively associated with Repaired Trust.

H4: Repaired Trust is higher if a company discloses the breach immediately rather than delays reporting of breach.

RESEARCH METHDOLOGY

The research was conducted using an online, scenario-based survey. Subjects were recruited from undergraduate students at a Midwest university. The participants viewed a picture of an e-commerce website for a fictitious e-commerce company created specifically for this study. After viewing the website, subjects were asked a series of questions to assess their trust (T1: Initial Trust) in the e-commerce company. Next, subjects were asked to read a news scenario describing a data breach. Subjects were randomly assigned to either a news scenario that stated the company's management announced a data breach immediately after discovering it or a news scenario stating the company's management announced a data breach with a two-month delay. Trust in the website was remeasured after subjects had read the news announcement (T2: Violated Trust). Next, subjects were asked to read a second news scenario associated with a trust repairing activity—the provision of credit monitoring and identity theft protection. Their trust in the e-commerce company was remeasured (T3: Repaired Trust) after showing the second news announcement. Finally, the subjects were asked demographic information.

Subjects entered a personal identifying code to screen for participants who may have taken the survey more than once; no subjects completed more than one survey. To ensure that subjects were attentive in completing the survey, six attention check questions were spread throughout the survey. These questions asked subjects about the e-commerce company whose website they viewed as well as the content of the news scenarios. After removing subjects who had missing data or failed any of the attention check questions, the final analysis includes a sample of 202 usable observations for purposes of the analysis. The final sample included 96 males (average age 21.85 years, range 18 to 44 years, std dev 4.36 years), 103 females (average age 22.84 years, range 18 to 52 years, std dev 7.363 years), and three subjects who chose not to answer the gender question (average age 21.50 years, range 18 to 25 years, std dev 4.95 years). Subjects were almost evenly assigned by gender between the two cases (immediate versus delayed announcement of breach).

RESULTS AND ANALYSIS

The trust measure is a construct developed from the mean of four trust questions developed from extant studies (Bansal and Zahedi, 2015; Bansal, Zahedi, and Gefen, 2010; Gefen, Karahanna, and Straub, 2003). The same four trust questions were used to measure initial trust, violated trust, and restored trust. EFA analysis was conducted and the four items loaded on to their intended construct. Cronbach alpha values were above 0.70 composite factor reliability values were greater than .70. This supports the developed trust constructs and provides support for their convergent validity. Data was collected in three sequences (initial trust, violated trust, and repaired trust) which reduces the threat of common method bias (Podsakoff, MacKenzie, Lee, and Podsakoff, 2003).

The three trust measures (initial trust, violated trust, and repaired trust) were plotted for each of the two news scenarios—immediate versus delayed reporting of the data breach.

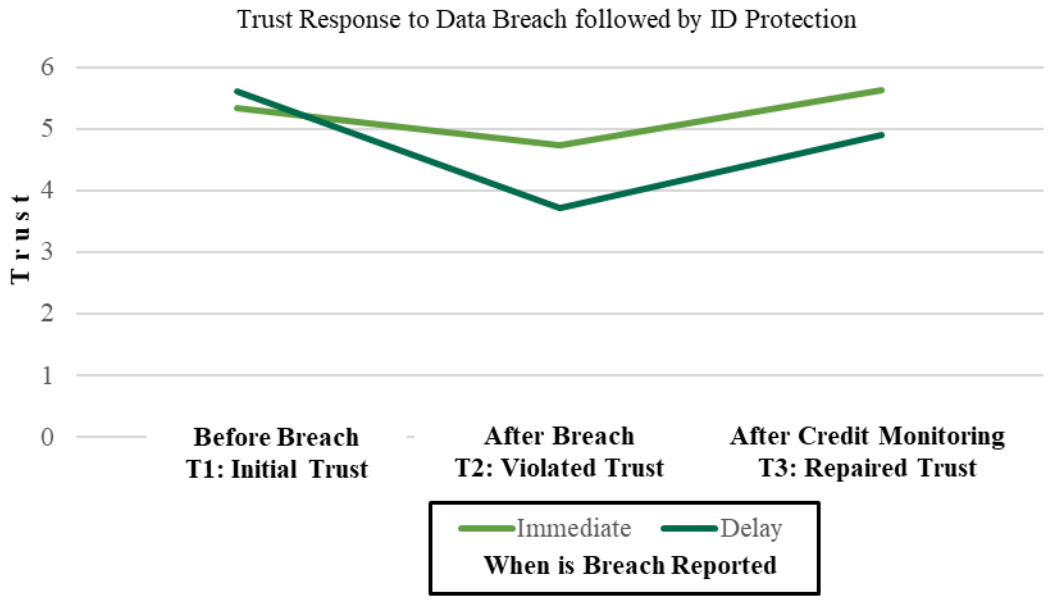

Figure 2. Plotting of Trust Across Two Scenarios

A paired sample t-test of initial trust and violated trust using the entire sample (both immediate disclosure and delayed announcement groups) showed that trust was significantly reduced after the data breach announcement (t=9.174, p=.000). This evidence supports H1. A second paired sample t-test of violated trust and restored trust showed that trust significantly increased after the news announcement that credit monitoring and ID protection would be provided, supporting H2 (t=-9.040, p=.000).

The paired sample t-tests were repeated for each group separately (immediate versus delayed announcement of the breach). The results were consistent with the tests using the entire sample; each group had significant decreases in trust after the data breach announcement and significant increases in trust after the announcement of credit monitoring (p-values $\leq$ .001). Thus, H1 and H2 are supported for both the scenario of reporting the breach immediately or the scenario where the breach announcement was delayed two months.

Between-subjects tests were conducted comparing the trust levels of subjects assigned to the immediate reporting scenario against the subjects assigned to the two-month delay in reporting the breach. The test was conducted comparing initial trust, violated trust, and repaired trust. There was no significant difference in initial trust between the two groups (F=.818, p=.367). This was the expected result as the experiment manipulation (timing of the announcement) occurred after measuring initial trust. The results comparing violated trust supported H3; the trust reported by the group that viewed the immediate reporting of the breach had significantly higher violated trust than the group that viewed the scenario where the company announced the breach two months after its discovery (F=11.736, p=.001). This result was consistent when comparing repaired trust; the repaired trust was significantly higher for the group that viewed the news that the company had immediately reported the breach (F=4.504, p=.035). This result supports H4.

Post Hoc Analysis

An observation drawn from the graph in Figure 2 is that repaired trust is comparable to initial trust. Paired sample t-test were conducted to test for the difference between initial trust and repaired trust. The findings of the paired sample t-test suggest that repaired trust is significantly lower than initial trust for the group

that viewed the news scenario where the company announced the breach two-months after its discovery (t=3.780, p=.000). There is no significant difference between initial trust and repaired trust for the group that viewed the news article where the company immediately disclosed the data breach (t=-1.266, p=.209).

CONCLUSION

The findings of the study help to understand consumers' reactions to e-commerce related events on the perceived trustworthiness of e-commerce companies and the timing of data breach announcements. The experiment results support all four hypotheses. This study extends the existing research by examining whether a company's forthrightness in announcing a data breach impacts trust reduction and subsequent trust rebuilding actions. The results suggest that companies that delay the announcement of a data breach are likely to suffer a larger drop in consumer trust than those companies that immediately disclose the data breach.

The post-hoc analysis suggest that companies that disclose the breach immediately upon its discovery may have an easier time repairing trust to the pre-breach levels. Consumers might perceive the act of withholding the information as untrustworthy. If an e-commerce company delays announcing a data breach, the damage might never be fully restored (Schwietzer, Hershey, and Bradlow, 2006).

This study has several limitations since the data were collected through a controlled experiment and used a population that consisted of only undergraduate college students. Another limitation of the study is the survey instrument included a picture of a website and related news articles for a fictitious company. The use of a fictitious company's website and news announcements about that company was necessary to examine how data breaches impact consumers' trust in e-commerce websites and how trust rebuilding efforts lead toward restoring trust. Future studies should look at the timing of actual data breach announcements and empirically examine the economic impacts of announcing data breaches immediately or with delay (e.g., stock price reductions or declining sales).

REFERENCES

1. Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 71, 62.
2. Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern. *European Journal of Information Systems*, 24(6), 624–644.
3. Choi, J., & Nazareth, D. L. (2014). Repairing trust in an e-commerce and security context: An agent-based modeling approach. *Information Management & Computer Security, 22*(5), 490-512.
4. Colquitt, J. A., Conlon, D. E., Wesson, M. J., Christopher, O. L. H. P., & Ng, K. Y. (2001). Justice at the millennium: A meta-analytic review of 25 years of organizational justice research. Journal of Applied Psychology, 86(3), 425-445.
5. Equifax Data Breach: Stock Price Falls as Criticism Mounts. (2017). *Fortune.com*, 16.
6. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90.
7. Identity Theft Resource Center (2017). *2017 Annual Data Breach Year-End Review*, Identity Theft Resource Center, California.
8. Jaeger, J. (2012). When to go public about a data breach. *Compliance Week*, 9(103), 38-39,66.
9. Kim, P. H., Cooper, C. D., Ferrin, D. L., & Dirks, K. T. (2004). Removing the shadow of suspicion: The effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of Applied Psychology*, 89(1), 104-118.

10. Liao, Q., Luo, X., & Gurung, A. (2009). Rebuilding post-violation trust in B2C electronic commerce. *Journal of Organizational and End User Computing*, 21(1), 60-74.
11. Lieber, R., & Cowley, S. (2017, September 26). Trying to Stem Fallout From Breach, Equifax Replaces C.E.O. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/26/business/equifax-ceo.html
12. Malhotra, A., & Malhotra, C. K. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research : JSR*, 14(1), 44.
13. Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal Of Marketing*, 81(1), 36-58.
14. McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, 38(1), 24.
15. Myung, K., Osei-Bryson, K., & Dorantes, C. (2009). Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms. *Information Resources Management Journal*, 22(2), 1-21.
16. National Conference of State Legislatures. (2018) *Security Breach Notification Laws*. February 6, 2018, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
17. Podsakoff, P. M., MacKenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
18. Ponemon Institute (2017), *2017 Cost of Data Breach Study: Global Analysis*, Research Report, Ponemon Institute, Michigan.
19. Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information and Computer Security*, 24(1), 73-92.
20. Schweitzer, M. E., Hershey, J. C., & Bradlow, E. T. (2006). Promises and lies: Restoring violated trust. *Organizational Behavior and Human Decision Processes*, *101*(1), 1.
21. Weiner, B. (1985). An Attributional Theory of Achievement Motivation and Emotion. *Psychological Review*. 92. 548-73.