Wait, Is This Dangerous For Me? Consumers' Reactions to Data Breaches That Pose (No) Risk to Them

Frederic Schlackl[1]
HEC Montreal,
Montreal, QC, Canada

Florian Pethig
Tilburg University
Tilburg, Netherlands

ABSTRACT

Data breaches lead to various negative reactions by consumers. However, prior research often is not explicit about if and how the studied consumers are affected by the data breach. For example, social media studies generally investigate the general sentiment by a large population of consumers, many of whom may not have a relationship with the breached company or be at risk from the breach, whereas compensation studies often investigate reactions by people who could be breached personally and thus face a risk from the breach. This study elaborates on the differences between these groups and uses a scenario-based pilot experiment ($n=95$) to differentiate reactions by consumers to a risky breach that could personally affect them from those to a non-risky breach that could not. We also provide a benchmark to establish the effect of hearing about a data breach compared against a clean control group.

Keywords: data breach, consumer reaction, news, experiment

INTRODUCTION

Data breaches have become increasingly common. Among consumers, such breaches trigger negative perceptual reactions such as feelings of anger, anxiety, and violation, as well as a decrease in the perceived reputation of the breached firm. In turn, these reactions can result in hostile behaviors such as negative word-of-mouth and reduced spending (Agarwal et al. 2024;

[1] Corresponding author. frederic.schlackl@hec.ca

Janakiraman et al. 2018; Martin et al. 2017). However, the literature examining reactions to data breaches generally overlooks how different groups of consumers are uniquely affected. It typically does not differentiate between customers of the breached company—who face a direct risk of their data being stolen—and non-customers, who, while aware of the breach, do not perceive themselves to be at personal risk. Data breach research often purports to capture general breach reactions, both from the public on social media (e.g., Bachura et al. 2022) and from people whose data is at risk (e.g., Hoehle et al. 2022). It is unclear whether people, when hearing of a data breach, primarily react to the breach as a corporate scandal, irrespective of whether it affects them, or whether they primarily react to the threat to their own data. Given the widespread concern about them in the business world (Dhillon et al. 2021), better understanding if and how consumers react to breaches that pose a risk to them (or not) is highly relevant for effective breach response planning and communication. It would also be helpful for guiding research, as the current literature on data breach effects is fragmented and often undifferentiated. We thus pose the following research question:

RQ: How do people react to hearing of a data breach that could personally affect them ("risky breach"), compared to one that poses no personal risk ("non-risky breach")?

In this work-in-progress paper, we use a scenario-based pilot experiment manipulating whether a fictitious data breach occurs at a firm that our respondents do business with, or at an unrelated firm. This project contributes to the data breach literature by measuring the effect of a breach on individuals to whom it poses are risk, and who thus fear for their data, as opposed to its effect on those who may mainly perceive the breach as a generic corporate scandal. It also establishes estimates of the treatment effect that hearing of a breach has on a person and allows for the comparison with a true control group—a novel approach in data breach research.

BACKGROUND

A growing body of literature studies data breaches and their effects on firms and individuals. Among its key findings are that data breaches have manifold negative effects, although more recent results challenge the extent and size of these effects. For firms, a temporary decline in stock market value after a breach has been reported, although this is subject to breach- and firm-specific characteristics (Ebrahimi and Eshghi 2022; Foerderer and Schuetz 2022). In general, data breaches have little to no effect on annualized firm returns and sales (Kamiya et al. 2021; Richardson et al. 2019). To the extent that effects exist, they appear primarily driven by reactions by customers of the breached firm.

Customers whose data has been breached exhibit reduced customer spending and spend less time on breached apps compared to their non-breached peers, although this effect generally fades within a few months (Agarwal et al. 2024; Janakiraman et al. 2018; Turjeman and Feinberg 2024). On social media, discussions of a data breach include expressions of anger, anxiety, and sadness over multiple stages (Bachura et al. 2022; Syed 2019), although it remains unclear how the social media users showing these reactions personally relate to the breached company. Beyond this, initial reactions are barely explored, as research generally studies such reactions as part of broader behavioral models that include effects of remedial actions of compensation and apology (e.g., Aivazpour et al. 2022; Choi et al. 2016; Goode et al. 2017; Hoehle et al. 2022; Masuch et al. 2021; Nikkhah and Grover 2022). Experimental studies on data breach response often manipulate these remedial actions or contextual factors such as data sensitivity or intentionality rather than the breach itself (e.g., Bentley and Ma 2020; Wright and Xie 2019). More importantly, there is generally no true control group without any knowledge of the data breach whose attitudes and perceptions can be compared to those hearing of the breach.

The overall impression gained from the literature is somewhat paradoxical. Data breaches have negative reputational effects on the breached company that manifest in a stock market decrease and negative social media sentiment (Bachura et al. 2022; Ebrahimi and Eshghi 2022). Simultaneously, there does not appear to be a long-lived impact on either consumer or firm outcomes (Janakiraman et al. 2018; Richardson et al. 2019), a disillusioning finding given that data breaches are perhaps the clearest manifestation of a company's failure to protect consumers' privacy. To better understand this apparent paradox, we seek to establish how exactly consumers react to a data breach that does not affect them—thus perceiving the breach more as a general scandal for the affected firm, and not perceiving any personal risk of data loss—in comparison to a data breach that could affect them and leads to a risk of their data being affected, which may engender risks such as fraud or identity theft. Understanding these reactions can help provide a stronger foundation to the relatively fragmented data breach literature.

METHOD

To investigate the difference between news of a data breach on consumers that could be affected by it and consumers that could not be, we conduct a scenario-based experiment. While scenario-based experiments are sometimes criticized for their low external validity, especially in an emotionally distressing setting such as a data breach, it is the most appropriate research design for the question at hand. Existing studies of data breach effects often use "opportunistic" data collection after a breach through surveys of potentially breached customers (Goode et al. 2017; Hoehle et al. 2022). While this provides great external validity, as respondents actually face the threat of a data breach, it lacks a true control group of customers that have not heard of the breach, thus making it difficult to estimate effect sizes. Respondents may also have different

amounts of information about the data breach prior to answering the survey. To maintain a clear control group and control over the information provided, the use of scenarios is necessary.

Table 1. Outcome variables of the experiment

Abbr.	Variable	Origin
ATTID	Attitude towards the company	Wright and Xie (2019)
PERINT	Perceived integrity	Deng et al. (2022)
PERCOM	Perceived competence	Deng et al. (2022)
PERBEN	Perceived benevolence	Deng et al. (2022)
COGTR	Cognitive trust	Martin et al. (2017)
SWIT	Switching intention	Choi et al. (2016); Nikkhah and Grover (2022)
NWOM	Negative WOM	Martin et al. (2017); Nikkhah and Grover (2022)
DISSAT	Dissatisfaction	Nikkhah and Grover (2022)
ORGREP	Organizational reputation	Bentley and Ma (2020)
ATTR	Attribution of responsibility	Bentley and Ma (2020)
VIOL	Emotional violation	Martin et al. (2017)

Outcomes of interest

We study a data breach's effect on constructs from prior literature on data breaches, trust, and privacy perceptions. These constructs are often tied to theoretical frameworks that view a data breach through different lenses (see e.g., Schlackl et al. 2022). Table 1 lists the variables used in the experiment. We capture the basic attitude towards a company (*bad, unfavorable, negative, … good, favorable, positive*), which is common in marketing research and was used by Wright and Xie (2019) in a consumer privacy context. As a data breach also is a trust violation, we measure trust through its three dimensions of perceived integrity, competence, and benevolence, in scales initially developed by McKnight et al. (2002) and Wang and Benbasat (2007) and notably used by Deng et al. (2022). We also measure cognitive trust (Martin et al. 2017). The intention to switch companies is a commonly observed variable in data breach research (Choi et al. 2016; Nikkhah and Grover 2022), as are negative WOM (Martin et al. 2017; Nikkhah and Grover 2022) and dissatisfaction (Bhattacherjee 2001; Nikkhah and Grover 2022). Organizational reputation and the attribution of responsibility are key constructs in public

relations research, where they were developed together with situational crisis communication theory (SCCT) (Coombs and Holladay 2002). Both these constructs and SCCT have been used in research viewing data breaches through a reputation and public relations lens (Bentley and Ma 2020; Syed 2019). To identify the emotional aspects of a data breach as a perceived breach of a psychological contract between the firm and the consumer, we also use emotional violation (Martin et al. 2017). We use 7-point Likert scales for all items. The items are omitted due to space considerations but are available from the authors upon request. As there is no consistent theoretical reason for why reactions would or would not differ for the different outcome variables, we decided not to develop explicit hypotheses.

Participants and Design

Figure 1 presents the experimental design. We used Prolific to recruit participants. The pilot experiment included 95 US adults (34 male, 54 female) who were paid 1.60 GBP for participation. The online survey software randomly assigned participants to one of three conditions (control, risky breach, non-risky breach) in a between-subjects design.

After the consent form, participants began by selecting the large American mobile service provider that they currently are a customer of (AT&T, Verizon, t-mobile, other). We opted for this industry, as its oligopolistic structure means that all major players are well known to the participants, including those that have never transacted with them, while products and services do not differ meaningfully between companies. Next, all participants except for the control group read a quick news bulletin stating that either their chosen company (risky breach), or one of the non-chosen

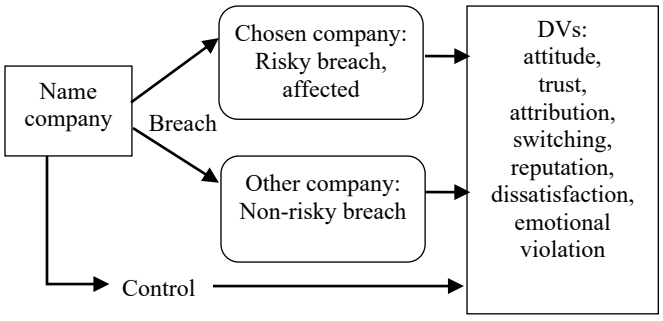

Figure 1. Experimental design

ones (non-risky breach) had recently faced a breach of its customer data and was investigating its full extent (e.g., risky: participants chooses AT&T, reads about breach at AT&T; non-risky: participants chooses AT&T, reads about breach at Verizon or t-mobile). Afterwards, participants in the control and risky breach conditions reported their answers to the variables from Table 1 for their chosen company, whereas participants in the non-risky breach condition answered the questions from Table 1 for the breached company (that they do not do business with).[2] Participants who chose "Other" (n=22) always were set to the non-risky breach category. Lastly, participants reported their control variables and basic demographic information such as age and gender.

RESULTS

Given the small sample size, we first used nonparametric Kruskal-Wallis equality-of-populations rank tests to assess whether there were differences in the distributions across groups. These results showed that there were significant differences between the groups for all dependent variables except NWOM. We further used t-tests to analyze differences between two groups (control vs. risky breach, non-risky breach vs. risky breach). We used Stata 18.5 for the data processing and analysis. Table 2 shows the preliminary results.

Surprisingly, there is nearly no difference between the control group and the group with the risky breach at their own company. After reading about a breach at their affected firm, consumers' attitude was slightly more negative, but none of the other variables showed any statistically significant difference. Given the large literature on negative impacts of data breaches, this is a puzzling finding. However, respondents had more negative impressions across

[2] Attribution of responsibility and emotional violation were not included for the control group, as the items did not make sense without a negative event (data breach) that they reference.

nearly all variables for the non-risky breach at the company they have no business relationship with, as compared to the breach at the company they do business with.

Table 2. Preliminary results

	Control		Non-risky breach		Risky breach		Control vs. risky breach			Non-risky vs. risky breach		
	Mean	SD	Mean	SD	Mean	SD	b	t	p	b	t	p
ATTID	5.57	4.52	3.23	1.70	4.71	1.66	0.86*	(2.20)	0.03	-1.48**	(-3.43)	0.00
PERINT	5.25	1.26	3.85	1.37	4.95	1.38	0.31	(0.94)	0.35	-0.99**	(-2.82)	0.01
PERCOM	5.72	1.03	4.10	1.58	5.51	1.04	0.22	(0.86)	0.40	-1.40***	(-4.14)	0.00
PERBEN	4.93	1.33	3.62	1.44	4.94	1.35	-0.01	(-0.02)	0.99	-1.32***	(-3.68)	0.00
COGTR	4.41	1.16	3.06	1.18	4.17	1.09	0.24	(0.88)	0.38	-1.11***	(-3.83)	0.00
SWIT	5.44	1.38	3.36	1.52	5.12	1.38	0.32	(0.95)	0.34	-1.76***	(-4.73)	0.00
NWOM	3.71	1.71	4.86	1.67	3.76	1.58	-0.05	(-0.13)	0.89	1.10*	(2.65)	0.01
DISSAT	4.79	1.30	3.72	1.52	4.84	1.30	-0.06	(-0.17)	0.86	-1.13**	(-3.12)	0.00
ORGREP	2.41	1.44	3.34	1.69	2.59	1.40	-0.18	(-0.52)	0.61	0.75	(1.90)	0.06
ATTR			5.08	1.11	4.18	1.27				0.90**	(2.92)	0.00
VIOL			4.59	1.71	3.14	1.69				1.45**	(3.34)	0.00
N	34		29		32							

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

Ex ante, it is unclear why this pattern occurs. It could be that consumers react more critically to a breach at a company they don't know closely; at the company of which they are a customer, other positive impressions could override the negative impression from the breach. However, it could also be that consumers' attitudes are more negative ex ante towards the other mobile service providers; consumers may have chosen their provider due to negative experiences with some of the others. This could particularly be the case since a large share of the respondents with the non-risky breach chose a non-top-3 mobile service provider and may be critical of the large providers. In future experiments, we intend to add a second control group of perceptions of other mobile service providers without a data breach to establish baseline values for the variables. We also intend to test the same variables for scenarios involving airlines and streaming services, as consumer perceptions could be contingent on the industry.

REFERENCES

Agarwal, S., Ghosh, P., Ruan, T., and Zhang, Y. 2024. "Transient Customer Response to Data Breaches of Their Information," *Management Science*, Mnsc.2021.01335. (https://doi.org/10.1287/mnsc.2021.01335).

Aivazpour, Z., Valecha, R., and Chakraborty, R. 2022. "Data Breaches: An Empirical Study of the Effect of Monitoring Services," *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* (53:4), pp. 65–82. (https://doi.org/10.1145/3571823.3571829).

Bachura, E., Valecha, R., Chen, R., and Rao, H. R. 2022. "The OPM Data Breach: An Investigation of Shared Emotional Reactions on Twitter," *MIS Quarterly* (46:2), pp. 881–910. (https://doi.org/10.25300/MISQ/2022/15596).

Bentley, J. M., and Ma, L. 2020. "Testing Perceptions of Organizational Apologies after a Data Breach Crisis," *Public Relations Review* (46:5), Elsevier Inc., p. 101975. (https://doi.org/10.1016/j.pubrev.2020.101975).

Bhattacherjee, A. 2001. "Understanding Information Systems Continuance: An Expectation-Confirmation Model," *MIS Quarterly* (25:3), pp. 351–370.

Choi, B. C. F., Kim, S. S., and Jiang, Z. (Jack). 2016. "Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems* (33:3), pp. 904–933. (https://doi.org/10.1080/07421222.2015.1138375).

Coombs, W. T., and Holladay, S. J. 2002. "Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis Communication Theory," *Management Communication Quarterly* (16:2), pp. 165–186. (https://doi.org/10.1177/089331802237233).

Deng, H., Wang, W., and Lim, K. 2022. "Repairing Integrity-Based Trust Violations in Ascription Disputes for Potential e-Commerce Customers," *MIS Quarterly* (46:4), pp. 1983–2014. (https://doi.org/10.25300/MISQ/2022/15679).

Ebrahimi, S., and Eshghi, K. 2022. "A Meta-Analysis of the Factors Influencing the Impact of Security Breach Announcements on Stock Returns of Firms," *Electronic Markets* (32), Springer Berlin Heidelberg, pp. 2357–2380. (https://doi.org/10.1007/s12525-022-00550-2).

Foerderer, J., and Schuetz, S. W. 2022. "Data Breach Announcements and Stock Market Reactions: A Matter of Timing?," *Management Science* (68:10), pp. 7298–7322. (https://doi.org/10.1287/mnsc.2021.4264).

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach," *MIS Quarterly* (41:3), pp. 703–727. (https://doi.org/10.25300/MISQ/2017/41.3.03).

Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., and Kude, T. 2022. "Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal Study of Target's Data Breach," *MIS Quarterly* (46:1), pp. 299–340. (https://doi.org/10.25300/MISQ/2022/14740).

Janakiraman, R., Lim, J. H., and Rishika, R. 2018. "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer," *Journal of Marketing* (82:2), pp. 85–105. (https://doi.org/10.1509/jm.16.0124).

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., and Stulz, R. M. 2021. "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms," *Journal of Financial Economics* (139:3), Elsevier B.V., pp. 1–31. (https://doi.org/10.1016/j.jfineco.2019.05.019).

Martin, K. D., Borah, A., and Palmatier, R. W. 2017. "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing* (81:1), pp. 36–58. (https://doi.org/10.1509/jm.15.0497).

Masuch, K., Greve, M., and Trang, S. 2021. "What to Do after a Data Breach? Examining Apology and Compensation as Response Strategies for Health Service Providers," *Electronic Markets* (31:4), Springer Berlin Heidelberg, pp. 829–848. (https://doi.org/10.1007/s12525-021-00490-3).

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334–359. (https://doi.org/10.1287/isre.13.3.334.81).

Nikkhah, H. R., and Grover, V. 2022. "An Empirical Investigation of Company Response to Data Breaches," *MIS Quarterly* (46:4), pp. 2163–2196.

Richardson, V. J., Smith, R. E., and Watson, M. W. 2019. "Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches," *Journal of Information Systems* (33:3), pp. 227–265. (https://doi.org/10.2308/isys-52379).

Schlackl, F., Link, N., and Hoehle, H. 2022. "Antecedents and Consequences of Data Breaches: A Systematic Review," *Information & Management* (59:4), Elsevier B.V., p. 103638. (https://doi.org/10.1016/j.im.2022.103638).

Syed, R. 2019. "Enterprise Reputation Threats on Social Media: A Case of Data Breach Framing," *Journal of Strategic Information Systems* (28:3), Elsevier, pp. 257–274. (https://doi.org/10.1016/j.jsis.2018.12.001).

Turjeman, D., and Feinberg, F. M. 2024. "When the Data Are out: Measuring Behavioral Changes Following a Data Breach," *Marketing Science* (43:2). (https://doi.org/10.2139/ssrn.3427254).

Wang, W., and Benbasat, I. 2007. "Recommendation Agents for Electronic Commerce: Effects of Explanation Facilities on Trusting Beliefs," *Journal of Management Information Systems* (23:4), pp. 217–246. (https://doi.org/10.2753/MIS0742-1222230410).

Wright, S. A., and Xie, G. X. 2019. "Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations," *Journal of Business Ethics* (156), Springer Netherlands, pp. 123–140. (https://doi.org/10.1007/s10551-017-3553-z).