AN EMPIRICAL INVESTIGATION OF COMPANY RESPONSE TO DATA BREACHES

Journal:	*MIS Quarterly*
Manuscript ID	2019-RA-16609.R2
Category:	Research Article
Keywords:	cybersecurity, data breach, response strategy, data breach notification laws, response time

SE's Comments	Our Response
Thanks for your revision, which has been received generally well by the AE. The AE and I agree that the paper needs major revisions, however, I would add that the "major" here does not reflect a risky revision, just a laborious one. I engaged the same AE as before, who managed to obtain four reviews from those who served previously in the first version. I must say that I consider this the finest AE report I've ever received, and agree completely with the advice with some very minor exceptions. His advice on the importance (or unimportance) of certain reviewer comments exactly reflects my thinking. The AE did ask that I provide guidance on page cutting, which will itself take much time. My cutting guidance appears below. I made an inquiry to Editor in Chief Andrew Burton Jones about page lengths and responded as follows: - The page lengths have indeed been reduced to 55 but that did not occur until after this paper was first submitted. - He recommends trying hard to reduce it to "60 pages or so" if it cannot be reduced to 55. - External repositories (such as on-line appendices) were eliminated late in 2020 but a new policy that takes effect in 2022 will re-enable the use of on-line repositories. He encourages you to make use of them in advance of new sweeping guidelines coming soon from Andrew and his team. The full text of that advice about your paper is shown below. Andrew's email in reference to reinstating the use of online appendices: "This policy will only come into effect on Jan 1 but we are encouraging authors and editors to opt-in to the process to the extent that they are willing. I'm not sure if you have used https://osf.io/ for any of your research, but it's an excellent external research repository. Rather than ask authors to delete the material entirely, they could simply create an external repository and move the material to that repository in an anonymous form and then just include the link. In the new policy, we don't feel that this link needs to be made available to the reviewers – but you and the AE could look over it.	Thank you for giving us the opportunity to revise the paper. We are pleased that two reviewers were satisfied with our responses in the prior round, and we found the comments of the other two reviewers incredibly useful to improve the paper. As SE mentions, the AE provided a fine report and gave us fabulous recommendations to improve the paper. We are excited about seeing the paper potentially advance in the review process. While shortening the paper was a challenge, we appreciate the SE for providing clear guidelines on how we could do this and for contacting EIC for further guidelines. Broadly, we have made these key changes to the paper in this revision: 1. We shortened the paper (cut 37 pages) to make it 60 pages with recommendations we received from SE and AE. 2. We further conceptualized investor's decision-making behavior by reviewing 84 studies from behavioral finance research. 3. We collected new data from Compustat to assess annual company revenues and further support Study 3.

As SE, you can simply decide which material is important for the paper and the review process (which you would then encourage to get into a reasonable number of pages) and which information is really just for future readers who want to learn more details about the paper and can be hosted online at OSF or another repository. The advantage of an external repository like OSF is that it has standard features for ensuring the preservation of the material in its original form."	
Regarding cuts recommended by the AE Treatment of Appendices: - A - CUT: make it available somewhere else, such as a contribution to a working paper series that can be downloaded or an external repository as Andrew suggested above. - B - ok; leave in - C - CUT: Not needed. It is redundant of material in the paper, although it only saves a page. - D - Leave in - E - Leave in - F - Leave in, contrary to the AE's recommendation. It's only one page and it's important to many readers. - G - CUT: Write a short paragraph summarizing this and make it available in an external repository - H - CUT: see G - I - CUT: See G - J - Leave in - K - Leave in, but perhaps shorten it	We created an account on https://osf.io (as suggested by EIC) and made several appendices available there, per SE suggestions. We made the links of each document publicly available and made our account anonymous. For each of such appendices, we inserted the link in the appropriate places in the paper. However, after moving several appendices to an external repository and removing Tables and Figures (per SE suggestions), we needed to cut further. Thus, we shortened a few appendices but ensured the quality and value of these appendices would not be impaired. Here is the information about our treatment of appendices (which is quite consistent with your recommendations): Appendix A: Cut (moved to an external repository) Appendix B: Left in Appendix C: Cut Appendix D: Left in Appendix E: Left in Appendix F: Left in Appendix G: Shortened and the full version moved to an external repository Appendix H: Cut and summarized in the text under MGA section Appendix I: Shortened and the full version moved to an external repository Appendix J: Left in but shortened Appendix K: Left in but shortened
My guidance on other cutting advice from the AE - Yes, consolidate and shorten the literature review as the AE suggests.	1. We removed old Table 1 and shortened literature review. 2. We fine-tuned implications for research and practice.

- Table 1: This can be deleted, but it would be good to make sure that somewhere the bridge to the response strategies is not lost from the paper. These show up in the "Post-event" part of the table. The Pre-event and Event literature does not seem to be critical to the study. - Implications for research and practice can be shortened. Maybe shoot for saving a couple of pages. - Figure 1 is certainly not necessary as it merely repeats what is in the text, and even if it did not, the graph seems to be unidimensional given that there are no off-diagonal elements. Is accepting responsibility (the Y axis) really that different than [expressing] remorse (the X axis)? The Coombs graphic does not seem to provide any evidence of that. Saying we are sorry is like saying we are sorry we allowed this to happen. o I think the solution for the space crunch is just to list them in three groups in a bulleted list or short table. You could actually remove everything from pg. 5, line 13, starting at "First" and extending to pg. 6, line 28. Replace the figure with a table that lists in the first column the category (Defensive, Moderate, and "acommodative"), in the second column each of the strategies, and then in the third column a short one-line definition. o See below for how it would look. It can replace that page-and-a-third of text. These are not difficult concepts to understand perhaps even just by reading the strategy names. o I believe the strategies are actually the groups and the tactics are the behaviors within the strategies. The Coombs paper might not agree but I believe that is the correct way to express these things. Label the columns as you see fit. Strategy Tactic Definition and/or short example (as you wish) Defensive Attack Accuser (definition/short example) Denial (definition/short example) Excuse (definition/short example) Moderate Justification (definition/short example) Ingratiation (definition/short example) Accommodative Corrective action (definition/short example) Full apology (definition/short example)	3. We removed Figure 1 and the description of strategies. Instead, we inserted (new) Table 1 that shows these strategies with their objectives, tactics, and definitions, as SE recommended.

Let's see where these cuts get you after some of the added items recommended by the AE and then we can regroup at that time. At this time I am not sure we will need the reviewers to take another pass but I will consult with the AE when we see your paper.	
Other Specific Comments Pg. 14, line 10: "negative reciprocates" with "reciprocates" as a plural noun doesn't seem to match definitions I've found. Do you mean "reciprocals" or "reciprocating impacts" or "reciprocated impacts?" Maybe a wording change to adopt a entirely different approach would be a good idea. Pg. 17, line 35: "value" not "valuate" Pg. 22, line 49: shouldn't it be "discussed how a factorial study" not "discussed how factorial study" Pg. 23, line 52: The company they actually used is not part of the study, but this section makes it sound like the actual company name is matched to the breach notification. This should be clarified to say that they were asked to think of a company to which they entrust their credit card data and then to imagine that the company suffered a breach. Pg. 25, line 3: "Ph.D." should be "Ph.D. degrees" or just say "doctorates" Pg. 43, line 8: Please DO NOT say the study "proves" anything. I will not approve this paper for publication if that phrase is used. A study does not prove, but it "shows" or "suggests" or "supports the notion that." Such a notion should be basic in any PhD program. We once decided not to hire a faculty candidate when he/she said that the data proved her hypothesis. It might be aggressive to suggest that the authors read some tutorials on falsifiability and/or the philosophy of research, and/or research methods, but such materials would be likely to cover that notion.	Thank you for these excellent suggestions. We revised and fixed these issues with your recommendations.

AE's Comments	Our Response
Thank you for this opportunity to review this revision of "An Empirical Investigation of Company Response to Data Breaches." This is an impressive revision and I now think that this paper contributes at the level of an MISQ article. I am recommending a major revision so that you can shorten the paper and finesse some theoretical arguments, among other things. I want to thank again the four reviewers for their time and expertise in evaluating this manuscript. I very much appreciate their willingness to help develop your research and support MISQ. The contribution of this paper is that it sheds light on two compelling current questions: 1. How should companies best respond to consumers and investors after a data breach? 2. What is the effect of timing on companies' response? Despite the clear importance of these questions, your expanded literature review shows that they have not been directly addressed in the past. Your newly expanded Study 1 is comprehensive, clearly documented, and nicely informs your theoretical model and the design of your factorial survey in Study 2. Although my concerns with the factorial survey from the previous round remain (e.g., common method bias; requiring respondents to simultaneously imagine: the company involved, their surprise, their dissatisfaction, their likelihood of spreading negative word of mouth (WOM) and switching to a different product or service), the fact that 85% of your respondents reported being compromised in at least one data breach meant that your scenario and treatments were personally relevant to respondents, making their reported intentions more meaningful than would be the case otherwise.	We really appreciate your guidance in the prior round and the way you have summarized and provided constructive guidance in this round. We are glad that our extended literature review underpins the importance of the research questions and Study 3 gives some insight on investor's behavior with respect to data breach responses. As guided by the SE and your comments, a large part of the challenge was to reduce the size of the manuscript to accommodate MISQ's revised guidelines. We have done that and the paper is now at 60 pages (all included) as recommended in the SE letter. We thank all four reviewers for their timely response and constructive feedback. We are pleased that reviewers 1 and 4 are satisfied with our effort to address their concerns. We recognize the importance of the remaining comments from reviewers 2 and 3 and worked diligently on their feedback (with the recommendations that we received from you). Please find our point by point response below.

More importantly, your new Study 3 does a very nice job of (1) showing how the accommodative response strategies and timing affect investors as an additional type of stakeholder, and (2) corroborating the findings of Study 2. I especially like that the moderating effects in your model apply to both Studies 2 and 3. Because your findings are consistent across Studies 2 and 3, this goes a long way in compensating for weaknesses in either method. Reviewers 1 and 4 are satisfied that you have addressed their concerns. Reviewers 2 and 3 are pleased with the progress you have made but still see issues that need addressing. I also see remaining issues, but I think these largely have to do with presentation and theorizing, which I describe below.	
Shortening the Paper MISQ's new maximum length guidelines for research articles are 55 pages, "including tables, figures, references and appendices" (https://misq.org/lengths). The manuscript is now at 97 pages not including the abstract page or response document. Besides being a new requirement, I think that the current length of the manuscript detracts from the paper overall. I recognize that fitting three studies within 55 pages will be a challenge, but I think the paper will be better for having a concise presentation. I also acknowledge that many of the appendices you have included in this round were in response to reviewers' comments. These appendices were helpful for the review process. I suggest that you now remove most of them to streamline the paper. I'll leave it to the senior editor to make definitive statements on what you show cut from the paper. However, here are some suggestions to consider: • Cut Appendices A: Literature Review, C: Constructs and Definitions, F: Demographics, H: Measurement Invariance Test	Thanks to the guidelines that we received from the SE (and his consultation with the editor-in-chief), and from you (as AE), we shortened the paper. Mostly all your suggestions have been followed regarding the Appendices and Figures. The current revision has 60 pages that meet the requirement of MISQ.

Results, Appendix I: Factorial survey post-hoc analysis, and possibly K: Event study post-hoc analysis and robustness test. • Consolidate and shorten the literature review for "crisis response strategies" and "data breach consequences and responses." • If needed cut, Table 1. • Your discussion section does a good job at discussing implications for research and practice, but this can be accomplished in four pages rather than seven. • Drop Figure 1 if needed.	
Theorize the behavior of investors R3 notes that besides for the direct effect (H2), you do not theoretically distinguish the behavior of investors and consumers. R3 makes an excellent suggestion that you either consolidate your hypotheses to predict customer and investor behavior together (e.g., combine H3 and H5, H4 and H6, and H7 and H8) by arguing their behavior should be the same, or that you differentiate the behavior of investors and consumers and offer theoretical explanations that are specific to investors in H6 and H8. I recommend that you take the latter route, as I agree with R2 that the behavior of investors and consumers are different. Although it is possible that some investors of a company may also be consumers of the same company's products or services, I think this is weak argument and unnecessary. Practically, this means you should add 1-3 paragraphs to theorize the behavior of investors before hypotheses H6 and H8, as you already do for H2.	Thank you for this great recommendation. We agree with you that second route (differentiation) could add more value to this paper and contribute more. So, we searched for "investor decision making" in Web of Science database and found 84 studies to review. After reviewing these studies that were mainly from behavioral finance research, we wrote two paragraphs before H4, H6, H8 (as you suggested) to explain (a) investors' specific characteristics and behaviors, and (b) how company responses and statements could affect investors' decision making. We also improved H2. We added these two paragraphs: "In addition to customers, investors are influenced by crises and following company actions. In this regard, behavioral finance research investigates investors' decision-making with respect to company responses. This research enumerates several characteristics specific to investors that differentiate them from other stakeholders. According to the axioms of utility theory, investors are (a) completely rational, (b) able to deal with complex choices, (c) risk-averse, and (d) wealth-maximizing (Nagy and Obenberger 1994). Recent studies have also argued that investors' behavior could be irrational (e.g., herd behavior) when access to real-time information is limited and investors have insufficient time for deliberation (Jackson and Orr 2019; Nigam et al. 2018). The irrational behavior could be triggered by crisis events such as terrorist attacks, earthquakes (Brounen and

	Derwall 2010), and data breaches (Martin et al. 2017; Yayla and Hu 2011), characterized by high uncertainty and inadequate information (Jackson and Orr 2019). In the light of irrational behavior and data breach crisis, prior research argued that investors could have emotional reactions to data breaches (Malhotra and Malhotra 2011). Although investor's decision-making could be affected by crisis events, research has found that company statements could manipulate investor's decision-making behavior. Positive or favorable information decreases uncertainty in the stock market and leads to stock price increase (Nigam et al. 2018). When the breached companies issue response letters that include favorable information about accommodative strategies, they signal the highest level of remorse to retain customers. As investors avoid uncertainty, customer retention ensures more stable future financial performance and lower associated costs (Anderson and Mansi 2009). Thus, investors reward company responses that have positive sentiments and signal stable financial performance in the future (Connelly et al. 2011; Teo et al. 2016)."
Test for decreases in revenue in Study 3 The SE stated in the previous round: If you do so [perform an event study], I would not recommend limiting this to only examining stock prices, as you state on pg. 38, but also to examine a downturn in revenue, and for what period. R2 echoes this suggestion saying that using revenues as the dependent variable could be used as a proxy for customer behavior. I suggest that in addition to using the measures cumulative abnormal return (CAR), buy-and-hold abnormal return (BHAR), and calendar-time abnormal return (CTAR) as dependent variables, that you also use revenue as a dependent variable. If revenues are also significantly affected, then this will more closely support Study 2.	Thank you for this recommendation. We agree with AE that analyzing revenues can shed light on the longevity of the data breach effect. We collected data on annual revenues from Compustat. We analyzed the average of annual revenues for three consecutive years: data breach year, and one year before and one year after the breach year. The results are consistent with long-term event study results and show that the effect of data breaches diminishes within one year. We added this paragraph to the post-hoc analysis as a footnote: "We also investigated the effect of data breaches on annual revenues. We collected data from Compustat but data for 12 companies in the breach years were not available. We compared the averages of three annual revenues: the year the data breach occurred (Y), one year before (Y-1), and one year after the data breach (Y+1). The ANOVA results [F (2, 461) = 0.39, p= 0.67]

I want to emphasize, however, that even if you do not find a significant change in revenues, the results for measures CAR, BHAR, and CTAR are sufficient for Study 3 to make strong contributions. In this case, I suggest leaving revenues out of Study 3 but just acknowledge in a footnote that revenues were also examined but did not change significantly.	show that there is not a significant difference among the three averages of annual revenues. In other words, data breaches did not significantly decrease the average of annual reviews in the breach year and the year after. These results, consistent with the findings of the long-term event study, show that the effect of data breach disappears in less than one year."
Guidance for responding to reviewers' comments I think the reviewers' comments are excellent and I suggest you address them as best you can. However, I want to offer guidance for how to respond to some specific comments. • I agree with R2 that this study can be viewed as using mixed methods because it has qualitative and quantitative components. However, since the qualitative analysis is only briefly mentioned in a footnote (Footnote 2, page 10), I recommend that you continue to call your methodology "multi-method." This will allow you to save space by not requiring the framing of a mixed-method study.	Thank you for this incredibly helpful guidance. Per your recommendation (and we concur), we continue to call our approach a "multi-method" study.
I second R2's suggestion to indicate in Figure 2 which hypotheses of the model are tested in which studies. For example, you could draw a line through the model or a box around the lower half of the model and add labels for Study 1 and Study 2.	Thank you for this comment. We agree that indicating what part of model is tested with what study would increase clarification. Therefore, we drew boxes and added labels, as you suggested.
• R2 comments: "I appreciate that you added Apology, Corrective Action, or Compensation in square brackets in Scenario B, Appendix G because this helps to understand and assess how you manipulated the various accommodative strategies. Accordingly, the manipulation of apology was "We apologize for what happened and we strive to maintain extensive security and privacy programs [apology]" (p. 73). I see this manipulation as problematic because, while the first part of the clause is the apology, the second part describes a remedial (or corrective) action (cf. Gwebu et al. 2020). I am afraid this description biased your results regarding the only-apology-case and, other than repeating the factorial survey, I am not sure how you could fix this."	Thank you. We also believe that it is not a flaw because (a) as the manipulation of "apology" and "corrective action" passed successfully, our respondents could distinguish between these two strategies with the presented statements; (b) almost all companies claim that they aim security and privacy practices but in the letters, we found specific actions that represent corrective actions. As we described in the prior response document, we found that corrective actions in the data breach notification letters include what the company does *specifically* about the happened data breach and what users should do. For example, there are two titles in the letters (please see the illustrative letter that we provided in the paper Appendix A): "What We Are Doing" and "What You Can Do". These titles represent specific corrective

I interpret "strive" in the present tense to mean that data security and privacy are ideals that the company always seeks to pursue. I don't see this as a statement of a remedial or corrective action. I therefore don't see a flaw that could have biased your results.	actions that could differ from data breach to data breach and striving to maintain security and privacy programs is just a broad goal of companies.
R2 comments: "In the manipulation check, you found a significant difference between early and late response time and concluded that the manipulation was successful. However, the mean of participants perception of early response time is M=2.94 on a scale from 1-7. Thus, there should be some participants who did not perceive the early response time-manipulation as early. To enhance reliability, I suggest to delete those respondents with M>=3 from the analysis." I think it is sufficient to show that participants in the early and late treatments had significantly different perceptions about the lateness of the response. However, if you optionally would like to test this further, you could simply remove those participants who answered one or two standard deviations away from the mean and compare the results with and without those respondents.	Thank you for this comment. We explored our data and found that about 4% of early respondents (about 2% of data) answered two standard deviations above the mean. We removed these responses and tested the model, but the main results did not change significantly. Thus, to keep the power of preliminary analysis (measurement model, MICOM, CMV, etc) and the main results (structural model, MGA) high as is, we decided not to remove them. Furthermore, the manipulation check of "time" passed successfully, which ensured us the robustness and validity of findings.
• R2 comments: "Although behavioral finance shows that if prices are going down, investors overreact and pull money out, I have doubts about whether this a valid measurement of the kind of actual behavior that you hypothesize based on EVT: "the dissatisfaction stemming from data breaches drives customers' and investors' reactions" (p.3). I wish that you include well-established references that clearly find stock market returns are good operationalizations of investors' actual behavior and thoroughly discuss it. Be also clear that you do not measure (but obviously assume) investor's dissatisfaction." This is a very good comment, as it can be inferred that investors also have perceived expectancy violations (PEV) and experience dissatisfaction, and thus sell off the breached company's stock.	Thank you for this valid point. Although we did not hypothesize the effects of perceived expectancy violation and dissatisfaction on investor's behavior, we believe that investors recognize data breaches as organization unexpected behavior, which leads to selling the stocks at lower prices. It is also consistent with prior research (Gwebu et al. 2018). As you recommended, in "Research Model and Hypotheses" section, we made a footnote and indicated it. Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," Journal of Management Information Systems (35:2), pp. 683-714. Additionally, as indicated earlier we have added two paragraphs on investor behavior based on the behavioral finance literature.

However, I am not sure you intend to make this argument. I note in Figure 2 that PEV and dissatisfaction are not involved in H2, H4, H6, and H8. I suggest that you state explicitly whether or not you think PEV and disappointment are involved for investors, even though you can't measure these variables in Study 3.	Here, we recognize that investors react based on uncertainty, and customer retention (through company statements) alleviates uncertainty. So, alleviating the extent of expectancy violation is implicit in investor behavior too.
I want to second R2's suggestion of introducing EVT before Study 1.	As you recommended, we introduced the EVT before Study1.
I think it is fine to call your model a moderated-moderated-mediated model before the method section, because I think this description can also describe a theoretical model.	Thank you. We also found that other studies (e.g., Gilal et al. 2018) used the moderated-moderated-mediation model to describe their theoretical model. Gilal, F. G., Zhang, J., Gilal, N. G., & Gilal, R. G. (2018). Association between a parent's brand passion and a child's brand passion: a moderated moderated-mediation model. Psychology Research and Behavior Management, 11, 91.
• R3 comments: "Then a natural question for firms is how to deal with these situations? I wonder whether the author can provide some perspectives about what new strategies firms can use to mitigate late responses' negative impact. Answering the questions may require extra effort in reviewing literature and designing a new factorial survey, but it can also add much value to the paper." I think this is an interesting idea, but I would leave this to future research given that this paper already involves three data collections and needs to be shortened.	It is a great comment and we had briefly discussed it in prior revision "Limitations and Future Research": "First, we only examined the set of accommodative strategies and contrasted them with no-action strategies because they were the only ones that breached companies adopted. However, future research can examine specific defensive (e.g., attacking the accuser) and moderate (e.g., justification) strategies to examine if these are more effective than accommodative strategies. Future research can also investigate why a company adopts a particular strategy (e.g., apology) and the challenges that a company faces when adopting a strategy. " However, we added this line in this revision: "As delayed responses have adverse negative effects, future research can investigate how to shorten the discovery time of data breaches and decrease the response time."
In your response document on page 2, you state: "We believe that average customers are not aware of the details of data breach notification laws. So, they do not know what state requires immediate, 30-day, or 45-day response. Moreover, these laws are for companies not customers, and many customers might not even know the location (state) of the company that they purchase from. So, we believe that it is just a perception of whether a response is late, even	We agree with you that it is useful to add this explanation in the paper. So, we explained it briefly in "Measurement Items" where we described how we measured response time (Appendix C). Here is the relevant part from the paper: "We believe that average customers are not aware of the details of data breach notification laws. Therefore, they do not know what state requires immediate, 30-day, or 45-day response. Moreover, these laws are for companies, not customers, and

legally. Finally, as you mentioned, we did a manipulation check. In the pilot study we found an issue with short response time as mentioned in the paper (we changed short response from 48 hours to 24 hours), we did not find any issue with long response time (i.e., 30 days). So, we feel confident that our treatment of delay was appropriately perceived. In the newly added event study, we used the difference between the announcement date and the response letter date as the corresponding moderating variable." I suggest you state this in the paper in a line or two.	many customers might not even know the location (state) of the company that they purchase from. Thus, we believe that it is just a perception of whether a response is late, even legally. We measured response time by providing early response time (24 hours) and late response time (30 days) in textual factors. We initially chose 48 hours for early response time because practice and research recommend an immediate response to the crisis (Coombs 2006; Hawthorn 2016; Matteson 2017) but the results of pilot study analyses showed that response time manipulation check did not pass successfully because the respondents did not perceive 48 hours as an early response time. Thus, we changed the response time to 24 hours for primary study and the manipulation check passed successfully. We also chose 30 days for a long response time because it is the minimum response time among the states that allow 30 to 45 days to respond. "
• Page 1, line 48: "to help the companies replenish the loss caused by the incident." Do you mean repair damage to their relationship with customers and investors?	Yes, we meant to repair the damaged relationships with customers and investors. We revised this line. Thank you.
The article includes citations to a number of technology and corporate blogs. Citing a few of these is okay, but I wonder if you can replace some with citations to high quality publications such as the NY Times, Wall Street Journal, Financial Times, etc. I acknowledge that some cybersecurity blogs are excellent sources of information, such as krebsonsecurity.com. Possible references to replace include: Davis, M. 2019. "4 Damaging After-Effects of a Data Breach," Retrieved from https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach. Hamilton, E. 2019. "The Importance of a Timely Data Breach Response," Retrieved from https://www.techtimes.com/articles/240760/20190402/importance-timely-data-breach- response.htm.	As you suggested, we removed several of these citations and added new citations from more credible sources such as Financial Times, NIST, IBM, and Gartner. We also updated the data breach statistics as recommended by Reviewer 4.

Hawthorn, N. 2016. "The First 48 Hours: How to Respond to a Data Breach". Retrieved from https://www.infosecurity-magazine.com/opinions/the-first-48-hours-respond-data. Kwan, C. 2020. "Equifax Direct Payments to Members to End Class Action Could Top $500 Million". Retrieved from https://www.zdnet.com/article/equifax-direct-payments-to- members-to-end-class-action-could-top-500-million. Montgomery, S. J. 2018. "People Decide to #DeleteFacebook Following Data Breach". Retrieved from https://www.complex.com/life/2018/03/people-delete-facebook-following-data-breach. Sanders, J. 2019. "Data Breaches Increased 54% in 2019 So Far," Retrieved from https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far. Skeath, C., and Kahn, B. 2019. "Round-Up of Recent Changes to U.S. State Data Breach Notification Laws". Retrieved from https://www.insideprivacy.com/data-security/data- breaches/round-up-of-recent-changes-to-u-s-state-data-breach-notification-laws. Temin, D. 2015. "You Have 15 Minutes to Respond to A Crisis: A Checklist of Dos and Don'ts," Retrieved from https://www.forbes.com/sites/daviatemin/2015/08/06/you-have- 15-minutes-to-respond-to-a-crisis-a-checklist-of-dos-and-donts/#5eb14e4e50a8. Zurier, S. 2018. "Consumers Are Forgiving After a Data Breach, but Companies Need to Respond Well," Retrieved from https://www.darkreading.com/operations/consumers-are- forgiving-after-a-data-breach-but-companies-need-to-respond-well/d/d-id/1333318.	
• In the last paragraph of page 2, link to a comprehensive article or authoritative website showing all US data disclosure laws, such as: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx	Thank you for this great point. We also think that a complete list of laws would help the readers to understand differences in data breach notification laws. So, we inserted the link you provided as a footnote in Introduction section.
• H2 reads:	Thank you for this great point. We agree with you that as we measured abnormal returns, it would be more appropriate to hypothesize CAR. So, consistent with prior event studies (e.g.,

"H2: When investors are informed about a data breach announcement, they react negatively toward the company in the stock market." Can you be more specific about investors' behavior? Similarly, H6 and H8 hypothesize about a "stock market reaction." Perhaps you could hypothesize about negative abnormal returns, since that is what you test.	Teo et al. 2016), we included CAR in the research model (instead of the market reaction) and revised H2, H4, H6, and H8 statements. We also updated H2 to include more relevant arguments about investor behavior in addition to information about investor decision-making that we included before H4 based on your prior comment. Teo, T. S., Nishant, R., and Koh, P. B. 2016. "Do Shareholders Favor Business Analytics Announcements?" The Journal of Strategic Information Systems (25:4), pp. 259-276.
• Page 10, line 29: Say "attorneys general," not "general attorneys."	We fixed it. Thank you.
• Page 70, line 49, "the letter includes all apology, corrective action, and compensation" Perhaps: "the letter includes all three accommodative strategies: apology, corrective action, and compensation."	We revised it as you suggested. Thank you.
• Page 5, last paragraph. I suggest creating a third category, "compensation." I think compensation could be seen as a form of apology, but it is qualitatively different and it would be helpful to distinguish at this point. You distinguish these three types later in the paper (e.g., p. 11, Figure 2).	As you recommended, we created a third category "compensation" in the literature review. SE recommended that we create a new Table instead of Figure 1, the new Table 1 shows compensation with a definition as a separate category of accommodative strategies.
• Istanbulluoglu is properly spelled with diacritics: İstanbulluoğlu (see https://twitter.com/doga_), so I suggest you add them.	Thanks. While in their paper even it was written Istanbulluogluas, we changed it to İstanbulluoğlu in this revision and now İstanbulluoğlu is consistent in the paper.
• Page 9, last paragraph. What about when a third party announces a data breach of another company and that company later sends a notification letter to customers? Following your description in this paragraph, would this be considered "no action"? Please clarify.	Thanks to your prior comment in the previous round to provide more information for Study 1, we accounted for "announcement date" and "response date". In the paper, we mentioned that (under Study 1): "While the announcement date is when the breach events are announced to the public, the response date is when the breached companies issue an official notification letter (that includes response strategies) to their stakeholders and legal parties. These two dates could be the same if the breached companies publicly announce their breaches by themselves and include their response strategies (e.g., compensation) in their announcements. " Regarding your comment on what about when

	a third party announces a data breach and the breached company sends a notification later, we recognized it and mentioned in the paper that "However, there are several cases in which there is no response date, or the response date is after the announcement date." So, when a company sends a letter after the announcement by a third party, it is an example of "when the response date is after announcement date". We argued further in the paper and posited that the fact that a third party announces a data breach could be an "intentional" or "unintentional" behavior of the breached company. This is the relevant part from the paper "It is usually unveiled when the breached company intentionally decides not to announce the data breach after the incident, and the announcement is made by a third party. Finally, the data breach could be announced by a third party while the company did not discover it and was unintentionally silent. " and we also wrote in the paper that "In this research, we recognize these last two cases as "no action" because the breached company was intentionally or unintentionally silent." However, to make this argument clearer, in this revision we add a parenthesis to this line "However, there are several cases in which there is no response date, or the response date is after the announcement date (breached company issues the response letter after the third party announces the data breach). "
• Please mention in the paper that 85% of respondents personally experienced at least one data breach.	We added this sentence at the end of "Data Collection Procedures: "We also found that 85% of respondents personally experienced at least one data breach event."
• Appendix G, "Therefore, this study does not suffer from common method variance." I suggest you say instead that these tests indicate that the risk of CMB is low, but that CMB remains a possibility given that these tests cannot rule out this threat.	We revised that as you suggested (new Appendix E). We also mentioned the possibility of CMV in the Limitations and Future Research section. Thank you.
On page 10, line 36 you mention 163 response letters. On page 31, line 22 you mention 166 response letters. Please clarify.	For Study 1 (content analysis of letters), we found 204 data breach announcements with respect to official response letters. We excluded 41 companies that adopted "no-action" and coded the rest 163 company responses. We have mentioned it in the paper in Study 1: "We finally used 204 data breach announcements with respect to official response letters from

	publicly traded companies that faced data breach incidents. We found that 41 companies adopted a no-action strategy. We read each response letter from the remaining 163 companies and analyzed the content of these letters to identify the adopted strategies " For Study 3 (event study), we kept no-action because we wanted to compare it with other strategies. So, we worked with 204 sample size that we collected in Study 1. However, as the event studies are subjected to confounding events, we used Lexis-Nexis database to find any confounding events. We excluded 38 observations because of confounding events and used the rest 166 for further analysis. We have mentioned it in the paper in Data Collection of Study 3: "we used the dataset of data breaches and official response letters that we collected for Study 1. However, the event study is subject to confounding events. As the hypotheses of this study require estimating longer event windows, we controlled for an array of confounding events from around −1 to +35, including dividend declarations, contract signings, earnings information, mergers, acquisitions, and utilizing new technologies (e.g., big data, cloud computing). We used the Lexis-Nexis business news database to identify the confounding events and dropped 38 announcements accordingly. Finally, we used 166 data breach announcements in conjunction with the corresponding response letters for further analysis. " However, to avoid confusion, in Study 1, we changed "163" to "remaining companies".
Thank you again for this excellent revision and I wish you the best of luck taking this research forward. You are welcome to ask me questions about this report through the SE.	We really need to appreciate AE for the guidance and feedback. AE's comments made the direction of this revision clear, which helped us to improve the quality of the paper with a better vision.
R1's Comments	**Our Response**

Thank you for another opportunity to read and review this work. I believe the authors have done a good job responding to the questions and comments I had in the previous round. They have addressed the issues raised about the introduction lacking a primer to the use of dissatisfaction and a moderated-moderated mediation model. I see that the authors have indeed expanded on the study's contributions to research. Especially through measuring a more objective DV (as suggested by the AE and other reviewers) and assessing both customers' and investors' reactions to breach responses. The knowledge around the effect of breach response strategies provided by this study contributes to research: (1) that a compensation strategy before and after data loss is effective for organizations – demonstrating a good connection with the information privacy research stream, (2) that a combination of compensation and apology strategies can have more impact than the three strategies combined (i.e., compensation, apology, and corrective action). Being able to introduce the event study in this study to examine the effect on stock prices and the duration of the effect/downturn is indeed a substantial modification (as suggested by the SE and AE). Finding results that are consistent with the customer stakeholders also adds to the contribution. Also, in response to my comment, the study now includes more convincing language for the importance of assessing response timing. Reading through the reporting of the data analysis results, it seems simpler and easier to digest. Some minor issues 1. Change Vence to Vance: "In Study 2, consistent with prior security and privacy research (e.g., Vence et al. 2015)," 2. On page 38: Consider changing, "Second, the EVT discusses" to "Second, the EVT argues"	Thank you for your constructive feedback in the prior round that helped us to enhance the quality of the paper. In this round, we fixed your two minor comments. Thanks again for helping us to improve the paper.

R2's Comments	Our Response
I read your revision with great interest. The biggest change is that you added a third study, an event study. This study assesses how the stock market returns of 166 firms changed after a data breach event to represent investors' behavior in response to data breaches. The most interesting outcome for me is that for about 6 months, a data breach event will substantially affect stock market returns. Overall, I find the paper has improved. I appreciate the effort you engaged in by extending the literature review and by following the SE's suggestion of conducting an event study. This strengthened the paper's contribution. After all, three studies contribute more than two. Nevertheless, I am still missing some kind of novelty or surprise—the 'spark' as the SE called it—to make a contribution worthy of a publication in one of our best journals. I also got the impression that the inclusion of the investors' perspective adds a lot of complexity to the study while it has not helped solve several of the issues raised in the previous round. I will detail my major issues in the following:	Thank you for carefully reading our paper and providing excellent feedback in prior and this round. AE guided us to address some of your comments. For the rest, we did our best to address the comments and improve the quality of the paper.
1 - Contribution Although you now analyze customers' and investors' reactions in the paper, you do so in two different studies, i.e., you use different predictors, different samples, measures, and study contexts. Therefore, I cannot see the difference between your studies and prior data breach studies that "distinctively examine either customers (e.g., Choi et al. 2016; Goode et al. 2017) or investors (e.g., Yayla and Hu 2011; Gwebu et al. 2018)." (p. 37/38). To actually contribute in the way you state "that customers and investors are similarly influenced by the same response strategies and times" (p. 38), you would need to study responses of customers and investors to the same strategies in one study. You may do that by either re-running the factorial survey with investors of a breached firm or do the event study with revenues, just as the SE recommended. A decrease in revenue of a breached firm should represent customers' actual behavior.	Thank you for this comment. AE made a comment that the fact that investors might be the customers of the company and react the same is a weak argument. Therefore, AE recommended that we need to further delineate investors' decision-making behavior by writing a few paragraphs before H4. We also believe that this delineation would add more value to our paper and to some extent distinguishes it from prior studies in this area—given prior studies distinctively examined either customers or investors. Thus, we searched for "investor decision making" in the Web of Science database and found 84 studies to review. After reviewing these studies that were mainly from behavioral finance research, we wrote two paragraphs before H4 (as AE suggested) to explain (a) investors' specific characteristics and behaviors, and (b) how company responses and statements could affect investors' decision making. Although we agree with you that conducting a factorial survey with customers and investors could provide new insights, such study may not examine investor's actual behavior in the stock

It may further help ease the assessment of your study's contribution. While tables A.1.1 and A.2.2 give me an interesting overview of the range of prior studies on data breaches and related phenomena, you could do a better job to emphasize the research gap. Currently, it is hard to dismantle the findings or understand the crosses in the cells. As you study the impact of different response strategies on customers' emotions and behavioral intentions and on investor behavior, you may cluster the identified articles by the response strategy studied, the consequence by and/or for whom, or further antecedents/moderators. Then you should enter concrete attributes, such as accommodative strategy, firm performance, or speed of announcement, respectively. This may help better highlight which one of those 93 studies studied similar constructs or related issues, and how and why exactly your study differentiates from those studies.	market in the breach years. Furthermore, event study allows us to examine investor actual behavior in prior years such as 2006 or 2009. As investors usually sell their stocks or buy new stocks from different companies, finding the investors of companies in prior years (especially breach years) is very difficult if not impossible. As AE suggested, we also examined annual company revenues in this revision. We collected data of annual revenues from Compustat. We analyzed the average of annual revenues for three consecutive years: data breach year, one year before, and one year after the breach year. The results are consistent with long-term event study results and show that the effect of data breaches diminishes within one year. With three empirical studies in this paper to examine specific accommodative strategies (tactics), conceptualizing investor's behavior and more importantly examining "time" with respect to response strategies along with post hoc analysis (long-term event study, company revenues etc.), we believe that this research could advance data breach research. Finally, in this revision we needed to cut 37 pages. SE kindly gave us a list of appendices that we needed to remove from the paper. Appendix A is removed in this revision but is moved to an external repository.
2 – Mixed-methods approach The increase in complexity may stem from the issue that study 3 is added, but not completely integrated. I sometimes got the impression that I was reading 2 papers in 1. To better integrate the three studies, I encourage you to frame the paper as mixed-methods study and carefully follow the steps of Table 4 in Venkatesh et al. (2016). Thinking through RQ, purpose, strategies, meta-inferences, and quality assessments may help you to get a clearer picture on how the three studies and their findings may get along together. I understand that you had some concerns about the sequential nature of your studies. Creswell (2003), though, shows different ways how components of a mixed-methods study may be interwoven. On a	It is a great point. Thank you. However, given three studies in this research and the urge to shorten the paper, AE asked us to keep the design as "multi-method". AE said "I agree with R2 that this study can be viewed as using mixed methods because it has qualitative and quantitative components. However, since the qualitative analysis is only briefly mentioned in a footnote (Footnote 2, page 10), I recommend that you continue to call your methodology "multi-method." This will allow you to save space by not requiring the framing of a mixed-method study."

final note, you do a mixed- not a multi-method study, as you state on p. 22, because you combine quantitative (studies 2&3) and qualitative components (study 1) (Venkatesh et al. 2013). Interestingly, though, the research model (Figure 2) completely integrates studies 1&2. I missed at least any hint that the model is analyzed/tested in two different studies and combines two different stakeholder perspectives or "two different dynamics", p. 22. Currently, for instance, without reading the text, it is unclear whether customers and/or investors are perceiving PEV & dissatisfaction. I suggest to separate Figure 2 into two models or draw at least a clear line between the customer and the investor components. To increase readability of your model(s), you may also use the common notion and present latent variables as ovals to differentiate them from observable variables (rectangles).	
3 – Hypotheses You should work on the line of arguments in most of your stated hypotheses: - H1: Dissatisfaction is a loss emotion (see Beaudry and Pinsonneault 2010). So, first of all, it may not rise "along with loss emotions" (p.10). Second, as far as I understand, you point this categorization out to justify your selection of dissatisfaction. The current discussion, however, (still) fails to explain why you selected dissatisfaction in favor for any other loss/negative emotion. Thus, you should be more clear in your reasoning.	We chose dissatisfaction over other loss emotions because customer complaining behavior research constantly found that after a service failure, dissatisfaction arises. Here is the relevant part of H1 argument that indicates why we chose dissatisfaction: "Along with emotions of loss, research on customer complaining behavior constantly finds that dissatisfaction is prompted by negative feelings towards a company when a service fails (Day and Landon 1977; İstanbulluoğlu et al. 2017; Kim et al. 2010). A data breach is an exemplar of a service failure (Goode et al. 2017) as the data breach violates customers' expectations of the company to protect their information. Thus, customers become dissatisfied with their relationships with the breached companies."
H2: You current argumentation is mostly based on the assumption that investors are also customers, but I would argue that this is rarely the case. Therefore, I would suggest to cut back this argument. I rather feel there are better arguments why investors "react negatively toward the company in the stock market". For instance, investors may anticipate expensive lawsuits and negative public image stemming from the data breach. In addition, investors may also experience negative emotions independent of whether they are also customers of the breached firm.	Thank you for this suggestion. We reviewed a few data breach event studies to get more ideas. Then, we revised H2 argument to include more relevant arguments regarding investors.

They are afraid to lose their money. See prior work, such as Gwebu et al. (2020), for more ideas.	
H3: • How can the knowledge we gain from prior studies be "limited" but at the same time serve to build your premises? So, you should re-think your choice of words. • H3 is a customer-level hypothesis and your argumentation is solely focused on behaviors and experiences of the responding company. Argue about how customers may perceive corrective action, apology, or compensation strategies and why those strategies will affect their behaviors.	Thank you for this great suggestion. We revised the line that included "limited". H3 and H4 are about the effect of accommodative strategies in a broad form (not specific strategies: i.e., corrective actions, apology, compensation). So, our arguments are about accommodative strategies in general. As mentioned earlier, we added two new paragraphs to discuss investor's behavior, which makes the argument to include both customer's and investor's behaviors.
H4: The same applies to H4. You need to argue about how the moderation will work, i.e., how accommodative strategies may influence investors' perceptions, emotions, and behaviors.	As mentioned earlier, we wrote two new paragraphs for H4 to include more discussions of investor's behavior and how investor's behavior is manipulated by company statements.
H5/6: I cannot see in Figure 1 that "providing compensation demonstrates a higher level of remorse and accountability (see Figure 1)". What I see in Figure 1 is that this is the case for apology. Apology may or may not include compensation (Coombs 1998). I can think of organizations that actually compensate customers without even displaying any signs of remorse or accountability for the data breach. Such compensating responses without apology may plead for a smaller effect than with apology. Moreover, what is the "best strategy among others"? In my view, there is either the best strategy, or not. Thus, overall, from your current argumentation, I do not understand why you expect compensation to have a higher impact than apology or corrective actions and this needs a better argumentation—especially, as the empirical results also do not support that.	We agree with you. Thank you. SE and AE recommended that we remove Figure 1 and we did so. However, we inserted new Table 1 and added compensation as a separate strategy per SE and AE recommendations. We revised H5-6 arguments accordingly. By "best strategy among others", we meant that prior research compared compensation with other strategies and found that compensation is the best strategy. However, per your comment, we revised that part and included this in H5-6 argument: "Compensation was posited to offset the customer's total cost (Grewal et al. 2008) and was found to be the best strategy in comparison with other strategies (e.g., Borah et al. 2020). "
4 – Major methodical issues • Study 1: I appreciate the expanded and more thorough description of the content analysis of response letters. From the 496 events, you found 204 response letters, among those you identified 41 with a non-action	According to the data breach notification laws, breached companies must notify affected people. They also need to submit a copy of notification letter to the general attorney of affected states. As described in Study 1, there is not a single source to find the letters. Thus, we collected letters from various sources including the websites of attorneys general, the breached companies' websites, security blogs, and online news websites.

strategy. What is unclear for me is on which fact or rule did you ground your categorization that those 41 firms adopted a non-action strategy? If I think of a “non-action” strategy, I would not expect those firms to hand out any response letter at all. And what about the remaining 292 events? Did you try to find those letters but they were not issued or have you not tried to find one for all of them? Furthermore, by design of study 1, you were not able to detect defensive or even purely moderate strategies because why should organizations publish a letter just to state that everything is fine? Hence, if organizations issue a response document, then they most probably used an accommodative strategy to respond to the data breach. Therefore, do not sell it as “insight” that you did not identify any defensive or purely moderate strategies because that is not what we expect to find. Rather, I suggest to frame it directly in the last sentence of p. 10: You coded the letters based on the types of accommodative strategy (i.e., not “based on the response strategies of Figure 1”, p. 10).	However, we could find information of only 204 announcements and letters (we were not able to find information of other 292 companies). Based on AE’s comment in the initial round, we provided more information about "no-action" strategy in Study 1. In short, we identified and described three situations that response date is after announcement day. In this regard, companies may adopt a "no-action" strategy intentionally (not responding) or unintentionally (responding much later, such as 30 days after the announcement date) and we described it in Study 1. Announcements information that we collected from Privacy Rights Clearinghouse, Databreaches.net, PHIPrivacy.net, and the US Department of Health and Human Services in many cases indicated whether the company responded or not. In other cases, we referred to the response letters that we collected. If we were not sure whether the company responded or not, we removed it from our dataset (those 292 companies that we could not find their information). Thus, with comparing announcement information and response information that both have "date", we could detect whether the company intentionally or unintentionally adopted a "no-action" strategy. We found 41 companies adopted "no-action" that include both intentional and unintentional doing “no-action”. Although we could add those "unintentional" responses to Table 2, we deliberately did not do that because those strategies might be influenced by a third party’s prior announcement (companies incentivize more after public knows about the breach from a third party source). Moreover, the purpose of Study 1 is just identifying various strategies and not the number of companies that adopt each strategy and the companies that unintentionally had "no-action" made similar responses as Table 1. Furthermore, after increasing 100 companies in the initial round to 204 companies in the second round of submission, we found that the pattern of strategy adoption is the same. Data breach notification laws require that breach companies notify affected people, but these laws do not require breached

	companies to adopt accommodative strategies. We agree with you that when companies issue a letter, they admit that data breach happened, and a defensive strategy is ruled out. We mentioned it in the paper in Study 1 as well. However, while breached companies notify affected people by issuing letters, they could adopt a *pure* moderate strategy such as justification. In fact, we found that many companies adopted moderate strategies but in conjunction with accommodative strategies. Prior conducting Study 1, we reviewed data breach studies and crisis management research and got familiar with various strategies. However, we had no idea what type of strategies would be included in the data breach letters. So, our initial attempt was reviewing the letters and coding based on the strategies mentioned in literature. We believe that the fact that accommodative strategies are adopted alone or in conjunction with moderate strategies is a new finding in this research area.
Study 2: • I appreciate that you added Apology, Corrective Action, or Compensation in square brackets in Scenario B, Appendix G because this helps to understand and assess how you manipulated the various accommodative strategies. Accordingly, the manipulation of apology was "We apologize for what happened and we strive to maintain extensive security and privacy programs [apology]" (p. 73). I see this manipulation as problematic because, while the first part of the clause is the apology, the second part describes a remedial (or corrective) action (cf. Gwebu et al. 2020). I am afraid this description biased your results regarding the only-apology-case and, other than repeating the factorial survey, I am not sure how you could fix this.	Thank you for this comment. Regarding this comment, AE mentioned "I interpret “strive” in the present tense to mean that data security and privacy are ideals that the company always seeks to pursue. I don’t see this as a statement of a remedial or corrective action. I therefore don’t see a flaw that could have biased your results." We also believe that it is not a flaw because (a) as the manipulation of "apology" and "corrective action" passed successfully, our respondents could distinguish between these two strategies with the presented statements; (b) almost all companies claim that they aim security and privacy practices but in the letters, we found specific actions that represent corrective actions. As we described in the prior response document, we found that corrective actions in the data breach notification letters include what the company does *specifically* about the happened data breach and what users should do. For example, there are two titles in the letters (please see the illustrative letter that we provided in the paper Appendix A): "What We Are Doing" and "What You Can Do". These titles represent specific corrective actions that could differ from data breach to data breach and

	striving to maintain security and privacy programs is just a broad goal of companies.
• You should have deleted 2 scenarios from the universe because analyzing response time is only logical/plausible in combination with any strategy. So, please change the current reason that states "the direct effects of response time were not the purpose of the study".	Thank you for this suggestion. A factorial survey allows to have several dimensions and we could have a dimension with two levels for response time. However, we agree with you that we could provide a better explanation to avoid possible reader's confusion. As you suggested, we revised that part and included it in the Scenario Design section: "as we needed to analyze the effects of response times only in conjunction with response strategies, we eliminated two conditions of response times (their direct effects) in our scenario design".
• In your first round, you did not talk about a pilot study. So if you did this study subsequently to strengthen the selection of your analyzed response time, you should be faithful and could describe it as a post-hoc study with the purpose of expansion (Venkatesh et al. 2016).	We talked about the pilot study in the first round (page 23 line 3).
• In addition, how did you approach the 110 people of the pilot study, again via CloudResearch? And how did the sample look like in terms of demographics? Please also provide more information why, the response time manipulation check required us to change the early response time from 48 to 24 hours for the primary study." (p. 25); how did this manipulation check look like?	Yes, we collected pilot study data from CloudResearch and the requirement to participate in this study was being an adult over 18 years of age who provides personal information to purchase products/services from retail outlets. We checked our pilot study data and found similar demographics as the primary study. Females (52%) and Males (48%) (females were slightly higher in the pilot study than in the primary study). Education: high school or college (36%), bachelor (57%), master (5%), doctorate (2%). Age: 18-24 (15%), 25-29 (18%), 30-39 (30%), 40-49 (25%), 50-59 (6%), 60 and over 60 (5%). [percentages are rounded, and other demographic information is available upon request]. The manipulation that did not work was "After only 48 hours of the data breach event, the breached company provides the following response". It did not work with the same manipulation question because the respondents did not perceive it as early. We changed it to 24 hours, and it worked. We mentioned it in Appendix C.
• At the risk of repeating myself, it would be more consistent with H7, if you tested for the difference between early and late accommodative response strategies, instead of the difference between early/late response time and no action because in my view, you hypothesize it exactly that way: "H7: Response time impacts	We compared groups for testing the moderating effects because this the appropriate approach when the moderator variable is a discrete variable (Eberl 2010; Henseler 2007; Sarstedt et al. 2011). For H3, we hypothesized that accommodative response strategies moderate the effect of dissatisfaction on the outcome

moderating effect such that with early response time, the moderating effect of acc. strategies is stronger" that is, stronger than with late response time, not stronger than no response. Note that in study 3, you also compare early and late responses to derive an assessment about H8.	variables. To test this, we compared dissatisfaction->outcome in two groups: in no-action (control group) and accommodative (Table 6). H7 hypothesizes that this moderation effect becomes stronger in early response. To test this hypothesis, we broke down accommodative strategies into early response and late response. We tested this hypothesis with the same logic that we did for H3. We compared (early response vs no action) and (late response vs no action) (Table 6). We believe that we needed to compare early response vs late response *only if* we wanted to say the effect of early is stronger than late (which is not our intention). However, thanks to your comment, we found that the way we wrote hypothesis statements H7,8 might give a wrong impression. Thus, we tweaked the language of hypothesis statements for H7 and H8. Instead of saying with the early response, the moderating effect is stronger ("is stronger" might confuse readers that we wanted to say it is stronger than the late response), we wrote the following statement: H7: Response time impacts the moderating effect of accommodative response strategies on the relationship between dissatisfaction and customer's behavior (i.e., switching behavior, and negative WOM), such that early accommodative responses affect that relationship more than late accommodative responses. We did the same for H8. We also added more information about it in Study 3 in this revision: "Table 10 shows that while the means of the CARs for early response events are small and insignificant, those for late responses are large and significant. For example, the mean of CAR for late responses (−1, 35) is −2.64%. As the means of CARs for no action and late response are negative and significant (Table 8 and 10) but the mean of CARs for early response is insignificant (Table 10), we could conclude that early response decreases the negative effect of announcements on CAR more than late response. Response time

	affects the effectiveness of accommodative response strategies. Thus, H8 is supported." Eberl, M. 2010. "An Application of PLS in Multi-Group Analysis: The Need for Differentiated Corporate-Level Marketing in the Mobile Communications Industry," in Handbook of Partial Least Squares, V. Esposito Vinzi, W. W. Chin, J. Henseler, and H. Wang (eds.), Berlin: Springer, pp. 487-514. Henseler, J. 2007. "A New and Simple Approach to Multi-Group Analysis in Partial Least Squares Path Modeling," in PLS'7:The 5th International Symposium on PLS and Related Methods, Ås, Norway, September 5-7, pp. 104-107. Sarstedt, M., Henseler, J., and Ringle, a M. 2011. "Multi-Group Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results," Advances in International Marketing (2), pp. 195-218.
• In the manipulation check, you found a significant difference between early and late response time and concluded that the manipulation was successful. However, the mean of participants perception of early response time is M=2.94 on a scale from 1-7. Thus, there should be some participants who did not perceive the early response time- manipulation as early. To enhance reliability, I suggest to delete those respondents with M>=3 from the analysis.	Thank you for this consideration. Regarding this comment, AE mentioned "I think it is sufficient to show that participants in the early and late treatments had significantly different perceptions about the lateness of the response. However, if you optionally would like to test this further, you could simply remove those participants who answered one or two standard deviations away from the mean and compare the results with and without those respondents." We explored our data and found that about 4% of early respondents (about 2% of data) answered two standard deviations above the mean. We removed these responses and tested the model, but the main results did not change significantly. Thus, to keep the power of preliminary analysis (measurement model, MICOM, CMV, etc) and the main results (structural model, MGA) high as is, we decided not to remove them. Furthermore, the manipulation check of "time" passed successfully, which ensured us the robustness and validity of findings.
• The MANOVA in Appendix G for the group that received "apology only" showed significant differences between each pair of	Yes, the mean of apology is higher than the means of corrective action and compensation in apology group. Every pair in the

response strategies. But for "apology only", if the manipulation works, I would expect the responses to the pair 'corrective action and compensation' to show relatively equal means in the direction of "strongly disagree" (i.e., support of HO).	sentence "the results of MANOVA show significant differences between every pair of the three response strategies" means two by two between, for example, apology vs corrective action and apology vs compensation in apology group. In apology group, we did not report the test of corrective action vs compensation because we manipulated apology and we had to report its results. Per your comment and avoid confusion, we revised that line. SE also recommended that we shorten that Appendix. Appendix E has information about manipulation check in the revised paper.
Study 3: I am not an expert in event studies. My review and issues are therefore based on my basic knowledge of financial market analysis and some initial research. • Please provide more information about - which stock exchanges you used to collect stock prices and market index data of the breached firms and - why you chose the CAPM, if the market model works better for cross-sectional studies (cf. Martin et al. 2017)? • CAPM calculates the expected return. So, the formula in Appendix J should be E(R) = ..	Thank you, we already mentioned that we used CRSP stock price data set (previous round page 92 line 42; now is in Appendix F). We followed Yayla and Hu (2011 p. 68) to write the estimation method for our market model. As we used Eventus software to do event study, we found that the formulas of Yayla and Hu (2011) and market model of Eventus software manual are consistent (http://www.eventstudy.com/Eventus-Guide-8-Public.pdf) [please refer to page 73 of this manual]. We also conducted Fama-French model estimation (three-factor and four-factor) for the robustness check (Appendix G) and the results are consistent. However, we removed the formulas from the paper because we needed to shorten the paper and we already mentioned Eventus software in the paper and interested readers could find publicly available manual for more information. Moreover, as event study is a well-established method, many papers do not go through the formulas of estimation method (e.g., Benaroch and Chernobai 2017; Martin et al. 2017). Benaroch, M., and Chernobai, A. 2017. "Operational IT Failures, IT Value-Destruction, and Board-Level IT Governance Changes," MIS Quarterly (41:3), pp. 729-762. 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.
Why did you use so many different event windows? The market should incorporate data breach information quickly and I also do not see huge differences in the results (Table 7). I recommend to refer to other studies (e.g., Martin et al. 2017) and select event windows from -1 to	We found that almost not every two "event studies" including data breach studies used exactly the same event windows. Please compare the event windows of these data breach event studies:

+1 days (the show the strongest effects, see Table 7) around the event to calculate abnormal returns.	Benaroch and Chernobai (2017): [-1, 0], [-1, 1], [-1, 2], [-1, 3], [0, 1], [0, 2], [0, 3] Hovav et al. (2017): [-1,0], [-1,1], [-1,5], [-1,10], [-1,25] Richardson et al. (2019): [-120, 5], [-1, 3], [-1, 21], [-1, 63], [-1, 126] Martin et al. (2017): [0, 0], [-1, 0], [0, 1], [-1, 1] Our study: [-1, 0], [-1, 1], [-1, 2], [-1, 3] (Table 8 shows that all these event windows provide consistent results) The logic behind these event windows is that the stock market may have "pre-announcement" information about the data breach and may react before the market closes a day before the public data breach announcement (Hovav et al. 2017). We followed this logic in our research. Benaroch, M., and Chernobai, A. 2017. "Operational IT Failures, IT Value-Destruction, and Board-Level IT Governance Changes," MIS Quarterly (41:3), pp. 729-762. Hovav, A., Han, J., and Kim, J. 2017. "Market Reaction to Security Breach Announcements: Evidence from South Korea," ACM SIGMIS Database: the DATABASE for Advances in Information Systems (48:1), pp. 11-52. 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. Richardson, V., Watson, M. W., and Smith, R. E. 2019. "Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches," Journal of Information Systems (33:3), pp. 227-265.
Was it possible in your sample that the same firm can have multiple breaches? If so, how did this influence your calculations?	Thank you for this great comment. Our research investigates the effect of response strategies on customers and investors. While there are several companies in our dataset that had multiple data breaches, we found that their responses were mostly the same. We examined the effect of each of these strategies on CAR separately in the years that the data breaches happened. Although decisions on choosing response strategies might affect subsequent decisions, it is beyond the scope of our research to investigate it.

You found in Study 1, that several of the letters also integrated some moderated response strategies in addition to accommodative ones. While focusing on accommodative strategies only may not affect the results of study 1, additional moderate strategies in the letters could affect and bias your results in study 3. I therefore suggest to control for the effect that additional moderate strategies could have had.	Thank you for this comment. Although there might be additional information in letters (e.g., pieces of information that convey moderate strategies). However, individuals are not aware of this categorization and they behave based on their "perception" of nuances in the letters. According to crisis management research and service recovery research (e.g., Coombs 1998), accommodative strategies show a higher level of remorse and accepting responsibility which is more impactful on an individual's perception and behavior. Thus, we believe that with the presence of accommodative strategies with lower-level strategies (i.e., moderate strategies), the effect of accommodative strategies dominates that of moderate strategies. For example, if a company gives compensation (accommodative strategy) and justifies the breach (moderate strategy), it is compensation that drives an individual's behavior. We do not believe that the inclusion of accommodative strategies and moderate strategies in a single letter has additive effects. In fact, post-hoc analysis of both Study 2 and Study 3 of our research shows that accommodative strategies do not have additive effects. Moreover, the results of Study 2 (that exclude moderate strategies) are consistent with the results of Study 3 (that might include moderate strategies). Thus, we do not believe that the results of Study 3 are biased due to the lack of controlling moderate strategies. Coombs, W. T. 1998. "An Analytic Framework for Crisis Situations: Better Responses from A Better Understanding of the Situation," Journal of Public Relations Research (10:3), pp. 177-191.
Overall, what you do in Study 3 is, you analyze the effect of response strategies and timing on a firm's abnormal stock market returns calculated by the market model that is, on firm performance (see Martin et al. 2017). What you imply is that stock market going up or down is representing investors' behavior. Although behavioral finance shows that if prices are going down, investors overreact and pull money out, I have doubts about whether this a valid measurement of the kind of actual behavior that you hypothesize based on EVT: "the dissatisfaction	Thank you for this insightful comment. Event study is a well-established method to examine investor's behavior in the stock market. Here are a few examples: 1. Teo, T. S., Nishant, R., and Koh, P. B. 2016. "Do Shareholders Favor Business Analytics Announcements?" The Journal of Strategic Information Systems (25:4), pp. 259-276.

stemming from data breaches drives customers' and investors' reactions" (p.3). I wish that you include well-established references that clearly find stock market returns are good operationalizations of investors' actual behavior and thoroughly discuss it. Be also clear that you do not measure (but obviously assume) investor's dissatisfaction. • In this vein, how can "investors show a poor market return performance"? (p. 15) My understanding is that investors may show a poor demand for stocks and stocks or returns may show a poor performance.	2. Kang, E., Ding, D. K., and Charoenwong, C. 2010. "Investor Reaction to Women Directors," Journal of Business Research (63:8), pp. 888-894. 3. Hawn, O., Chatterji, A. K., and Mitchell, W. 2018. "Do investors actually value sustainability? New evidence from investor reactions to the Dow Jones Sustainability Index (DJSI)," Strategic Management Journal (39:4), pp. 949-976. 4. Werner, T. 2017. "Investor Reaction to Covert Corporate Political Activity," Strategic Management Journal (38:12), pp. 2424-2443. However, we agree with you that investor's behavior needed a better conceptualization in our research. For this revision, we reviewed 84 studies about investor behavior and revised the argument of H2. As AE suggested, we also wrote two new paragraphs to explain (a) investors' specific characteristics and behaviors, and (b) how company responses and statements could affect investor decision making before H4.
Minor miscellaneous issues: • I suggest to introduce EVT before study 1	As you suggested, we introduced the EVT before Study 1. Thank you.
P.14: „moderated-moderated-mediation model" is a methodical description of the research model. This label along with Hayes' description appears inappropriate in the (theoretical) research model section.	Regarding this comment, AE commented: "I think it is fine to call your model a moderated-moderated-mediated model before the method section, because I think this description can also describe a theoretical model." We also found that other studies (e.g., Gilal et al. 2018) used the moderated-moderated-mediation model to describe their theoretical model. Gilal, F. G., Zhang, J., Gilal, N. G., & Gilal, R. G. (2018). Association between a parent's brand passion and a child's brand passion: a moderated moderated-mediation model. Psychology Research and Behavior Management, 11, 91.
P.23: "The participants of this study randomly received a different dimension with different levels based on response strategies and times" (p.23). Usually, participants randomly receive a different scenario with	Yes, thank you. As we have two dimensions (strategy and time), we revised that line.

different combinations of dimensions and their levels. So, did you mean a different strategy rather than a different dimension?	"The participants of this study randomly received different dimensions with different levels based on response strategies and times."
In the data analysis on p. 28 ff, you write H3a/b, H4a/b. Please also label your hypotheses with a/b respectively in the research model section.	Thank you for this suggestion. Per AE's comment in the prior round, we changed the labeling in hypotheses. H3a and H3b are changed to H3 akin to H4. We updated the text accordingly. We also provided Table 11 that shows the summary of results.
P. 38: "We used the Lexis-Nexis business news database to identify the confounding events and dropped events accordingly." You may have dropped observations, not events. • Figure 3 is hard to read. Please improve quality.	As you suggested, we changed "event". Following prior event studies (e.g., Gwebu et al. 2018; Teo et al. 2016) we used "announcement". Thank you. "We used the Lexis-Nexis business news database to identify the confounding events and dropped 38 announcements accordingly." Figure 3 is derived from Eventus software and we do not have much control on the quality of image. However, we made it larger in this revision to make it clearer. Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," Journal of Management Information Systems (35:2), pp. 683-714. Teo, T. S., Nishant, R., and Koh, P. B. 2016. "Do Shareholders Favor Business Analytics Announcements?" The Journal of Strategic Information Systems (25:4), pp. 259-276.
Table Appendix C, I suggest to adapt the definition of dissatisfaction to "perceived discrepancy between prior expectancies about the company's performance and perceived performance after data breach incident" Table Appendix C, please integrate in the definition of corrective actions who has taken those actions to include that, in your study, the concept consists of both what the company will do and what customers should do.	Thank you for this comment. SE recommended that we remove the old Appendix C that included definitions. We need to appreciate R2 for providing excellent inputs.
R3's Comments	**Our Response**
Thank you for the opportunity to review this revised manuscript. I appreciate the authors' endeavor in revising the paper. Also, I am impressed by the excellent and constructive comments provided by SE,	Thank you for your constructive comments in the prior round that helped us to improve the paper. In this round, you also gave us

AE, and all three other reviewers. The authors did a good job incorporating most comments and addressing a majority of issues. I can see substantial improvement in several aspects. First, the literature review and theoretical development part are more focused on the data security context. Second, the revised paper presents important details in study 1 and study 2. In particular, Study 2 considers more factors (e.g., data breach experience) and tests to show results' robustness. Third, the authors use actual behavior data (stock prices) to examine different response strategies' impacts. Although the paper improves in many aspects, there are still some issues that need to be addressed. I hope the below comments can help the authors to revise the paper in the new stage.	very useful comments. We attempted to address every single of your comments in line with the AE comments.
Firstly, it is interesting to discuss response strategies' impact on different stakeholders (i.e., customers and investors). I also agree that analyses on new hypotheses would expand the paper's contribution. However, the authors can do a better job in framing that part. In the revised paper, the authors discuss the differences between customers and investors first and then generalize them to one concept in developing the hypotheses (moderating effect), which does not make much sense. I suggest the author can go either way, consolidate hypotheses or emphasize the differences. - Consolidation: Instead of discussing customers and investors separately, the authors can use study 2 and study 3 to assess the generalizability of theories for several reasons. First, it is tricky to differentiate the customers and investors and then hypotheses them separately. As the authors mentioned in the paper, "some investors may also be customers of the breached company, and thus, their investment decisions are influenced by their relational judgments as investors and their negative behaviors based …" (page 17 line 50 – 55). Second, the authors' hypotheses for customers and investors are very similar. The results also show the similar impacts of response strategies on different stakeholders. Hence, it is reasonable to combine them in the theoretical framework. If the authors want to consolidate the results, they may need to generalize the commonalities shared by customers and investors when facing firms' data breach incidents. In that case, study 2 and study 3 can examine stakeholders' intentions and behavior,	It is an excellent point indeed. After adding Study 3 (actual behavior with event study), we decided to add "investors" as another stakeholder. We believe that examining two different stakeholders would contribute to cybersecurity and data breach research more. However, we agree with you that such examination also requires a better conceptualization. Regarding your two great options: "consolidation" and "differentiation", the AE recommended that we take "differentiation" option. Thus, to better understand investor's behavior, we searched for "investor decision making" in Web of Science database and found 84 studies to review. After reviewing these studies that were mainly from behavioral finance research, we wrote two paragraphs before H4, H6, H8 (as AE suggested) to explain (a) investors' specific characteristics and behaviors, and (b) how company responses and statements could affect investors' decision making.

respectively. A recent paper (i.e., Raithel and Hock 2021) about crisis-response adopts a similar strategy. - Differentiation: If the authors want to expand the contribution by investigating different stakeholders' responses, they may need to enhance theoretical development on the investor side. I observe that the authors only discuss the differences in the research gap part: "…… while customers pursue event-specific satisfaction (Saad Andaleeb and Conway 2006), investors are loss-averse and seek long-term returns (Barberis and Huang 2001; Fama 1998)." (page 8 line 43-50) I suggest the authors theorize investors' intentions and behaviors separately before H4, H6, and H8. The hypotheses might change or not based on theories, but the discussion would contribute to differentiate customers and investors as two types of stakeholders. Second, I agree with SE and AE that using observational data can add much value to the study. Unfortunately, the current analyses might not be able to achieve the goal because of a lack of clarity. The authors are advised to carefully check details (e.g., table number) and elaborate on most findings. Below are some specific issues. The authors are advised to fix all of them.	
Page 34, line 5: "The results of parametric and non-parametric tests (Table 2)." Wrong table number?	Yes, thank you. We apologize for this. After we extensively shortened the paper (cut 37 pages) with the SE's and AE's recommendations, a few figures and tables removed. We updated the table numbers and double-checked to ensure they have correct numbers.
The authors need to provide more details in the argument. "Table 8 shows while compensation is more effective than corrective action by itself, its efficacy is not better than that of an apology." (Page 34, line 8). I do not see obvious evidence in Table 8. If there is, please elaborate on it.	While corrective action has significant values, compensation and apology both have insufficient values. As a result, compensation is more effective than corrective action to cancel out the negative effect. However, as both compensation and apology have insignificant values, we are not able to conclude that compensation is more effective than apology. To make it clearer, we revised this part and mentioned it in the revised paper: "While corrective action only has a significant negative CAR (-0.96%, $p < 0.05$), the results of the parametric and non-parametric tests (Table 8) show that compensation and apology do not have significant effects on CARs. Table 8 shows that while compensation is more effective than corrective action

	only, its efficacy is not better than that of an apology as they both have insignificant values. "
Page 34, line 50: "The considerable difference between the means of the CARs for early and late responses indicates that the response time affects the effectiveness of response strategies." The result is unable to support the moderating effect of response time.	We found from prior research that when the moderator variable is a discrete variable (here Time), the comparison of effects is suggested. Per R2' suggestion, we changed the H8 statement: "Response time impacts the moderating effect of accommodative response strategies on the relationship between data breach announcement and CAR, such that early responses affect that relationship more than late responses." To test this hypothesis, like what we did for H7 and Study 2, we needed to compare three conditions: no-action, early response, and late response. Table 8 and results [t (164) = 1.98, p = 0.04] show that accommodative strategies can significantly decrease the negative effect that data breach announcements have on the CAR (supporting moderating effect of accommodative strategies). However, Table 10 shows that while the values of "Late Response" are negative and significant, those of "Early Response" are insignificant. Therefore, as no-action and late response have negative significant values (Table 8 and 10), but the early response has insignificant values (Table 10), we could conclude that accommodative response effectiveness is subject to whether it is provided "early" or "late". We hope this explanation is useful.
In Appendix K, Page 95, line 43: "Table K3 shows the result of sub-samples regarding …" should read "Table K4 shows the result of sub-samples regarding…" In Appendix K, Page 95, line 45: "Table K4 shows the new estimations for hypothesis 8" should read "Table K5 shows the new estimations for hypothesis 8".	Thank you for catching these. As mentioned in prior comments, we extensively shortened the paper. These Tables are not in the paper in the revised paper and have been moved to an external repository per SE suggestion.
The authors may use Tobin's Q as another measure in analyzing long-term impacts (Bose and Leung 2019).	We agree with you that there are several approaches to examine how a company is affected by a data breach. Following prior research, we used short-term event study (Benaroch and Chernobai 2017) and long-term event study (Barua and Mani 2018) for Study 3. However, the AE recommended that we test for the decrease in company revenues. To this end, we collected

	data of annual revenues from Compustat. We analyzed the average of annual revenues for three consecutive years: data breach year, and one year before and one year after the breach year. The results are consistent with long-term event study results and show that the effect of data breaches diminishes within one year. We added this paragraph to the post-hoc analysis as a footnote: "We also investigated the effect of data breaches on annual revenues. We collected data from Compustat but data for 12 companies in the breach years were not available. We compared the averages of three annual revenues: the year the data breach occurred (Y), one year before (Y-1), and one year after the data breach (Y+1). The ANOVA results [F (2, 461) = 0.39, p= 0.67] show that there is not a significant difference among the three averages of annual revenues. In other words, data breaches did not significantly decrease the average of annual reviews in the breach year and the year after. These results, consistent with the findings of the long-term event study, show that the effect of data breach disappears in less than one year." Barua, A., and Mani, D. 2018. "Reexamining the Market Value of Information Technology Events," Information Systems Research (29:1), pp. 225-240. Benaroch, M., and Chernobai, A. 2017. "Operational IT failures, IT value-destruction, and board-level IT governance changes," MIS Quarterly (41:3), pp. 729-762.
Third, the finding of the response time is interesting. According to the setting in the paper, if a firm responds to a security breach incident after stakeholders know it, none of the response strategies would be helpful in mitigating stakeholders' negative perceptions. However, delay responses are sometimes unavoidable. For one thing, many other groups, including hackers, government agencies, or security firms, may detect the breached data before the firm, and they may disclose the incident to the public. Also, it takes longer for firms with limited resources to investigate the incident before revealing more detailed information (Sobers 2020). Then a natural question for firms is how to deal with these situations? I wonder whether the author can provide	It is an insightful comment. Thank you. Regarding this comment, AE mentioned: "I think this is an interesting idea, but I would leave this to future research given that this paper already involves three data collections and needs to be shortened." We had briefly discussed it in prior revision "Limitations and Future Research": "First, we only examined the set of accommodative strategies and contrasted them with no-action strategies because they were the only ones that breached companies adopted. However, future research can examine specific defensive (e.g., attacking the accuser) and moderate (e.g.,

some perspectives about what new strategies firms can use to mitigate late responses' negative impact. Answering the questions may require extra effort in reviewing literature and designing a new factorial survey, but it can also add much value to the paper.	justification) strategies to examine if these are more effective than accommodative strategies. Future research can also investigate why a company adopts a particular strategy (e.g., apology) and the challenges that a company faces when adopting a strategy. " However, we added this line in this revision: " As delayed responses have adverse negative effects, future research can investigate how to shorten the discovery time of data breaches and decrease the response time. "
Fourth, it is easy to get confused on which hypotheses are supported and which are not. I suggest the authors use a table to present all results. The table should have at least three columns: hypotheses, conclusion (support or not), main evidence (or page number). Otherwise, the representation of results may weaken the readability and quality of the paper. Below are some examples of issues. - Page 28, line 52: "H3a and H3b are supported" should read "H3 is supported." - Page 29, line 12: "H4a is supported, but H4b is not supported." I do not see H4a and H4b. - Page 33, line 55: "H5 is supported" should read "H4 is supported". - Page 34, line 10: Based on line 8, I can see two main conclusions. First, compensation is more effective than corrective action by itself. Second, compensation is not more effective than an apology. Therefore, "H6a is not supported, but H6b is supported" should read "H6a is supported, but H6b is not supported".	Thank you for suggesting how to improve the presentation of results. We fixed the issues that you mentioned. We also considered the labeling of hypotheses that AE recommended in the prior round. Thank you for recommending adding a summary Table. SE and AE recommended shortening the paper extensively (cutting 37 pages) and it was challenging to add any new Table. However, we managed to insert a new Table in the paper (Table 11) in the Discussion section to summarize the hypotheses testing results. We also fixed the issue of H6a and H6b. Thanks.
Minor Issues - Page 8, line 42: "that response strategies" should read "those response strategies". - Page 22, line 24: "Vence et al. 2015" should read "Vance et al. 2015".	We revised that line. We also fixed Vance et al. 2015 citation. Thank you.
In sum, although there are some weaknesses in the current manuscript, I still think this study is interesting and would contribute to the literature and provide useful practical implications, assuming you can address the points above successfully. I appreciate your efforts to craft these	Like the prior round, we found your comments very helpful to enhance the quality of this paper. Thank you so much.

intellectual contributions and I wish you the best of luck in the process of revising this work.	
R4's Comments	**Our Response**
Thank you for doing such a thorough job addressing reviewer comments. You should be commended for a job well done. At this point my comments are relatively minor.	Thank you for all the useful comments that you made in the previous and this round. We found the comments very useful to improve the paper.
The introduction is dated. I recommend updating this with statistics from 2021 if possible.	Thank you for this suggestion. We updated data breach statistics to include 2020 and 2021 data in the Introduction section.
The text in some of your figures seems small and hard to read. Can these be a bit bigger?	SE and AE asked us to remove and change a few figures. The figure of "Cumulative Abnormal Returns" is an image by Eventus software and we couldn`t change the text of the picture but we made the image bigger. We tried to improve the quality of other figures to be clearer.
In table 5, what do 3 *s mean? It isn't present in the key.	Thank you. *** means $p < .001$ and we mention it under Table 5.
In table 10, I don't believe significance < .10 is necessary to note. I would call this not significant.	Thank you for this point. We found that in the event studies (e.g, Barua and Mani 2018; Benaroch and Chernobai 2017) $p < .10$ is considered significant and we just wanted to be consistent with other event study papers. Barua, A., and Mani, D. 2018. "Reexamining the Market Value of Information Technology Events," Information Systems Research (29:1), pp. 225-240. Benaroch, M., and Chernobai, A. 2017. "Operational IT Failures, IT Value-Destruction, and Board-Level IT Governance Changes," MIS Quarterly (41:3), pp. 729-762.

AN EMPIRICAL INVESTIGATION OF COMPANY RESPONSE TO DATA BREACHES

Abstract

Companies could face serious adverse consequences in the aftermath of a data breach incident. To repair the damaged relationship with stakeholders after data breaches, companies adopt a variety of response strategies. However, the effect of different adopted response strategies on stakeholders' behaviors after a data breach is not clear. There are also differences in response time, which might be subject to individual state notification laws for beaches that occur in the U.S. As part of a multi-method study, we first identify adopted response strategies in Study 1 based on a content analysis of letters issued by companies (n = 204) following data breaches. These strategies include combinations of corrective action, apology, and compensation along with "no action". In Studies 2 and 3, we focus on customers and investors as the prominent stakeholders who are largely affected by data breaches. We present a moderated-moderated-mediation model based on expectancy violation theory. In Study 2, we design a factorial survey with 15 different conditions (n = 811) and we conduct an event study (n = 166) in Study 3 to examine the effects of response strategies and response times on customers and investors, respectively. The results indicate moderating effects of certain response strategies and, surprisingly, compensation is not found to be more effective than apology. The magnitude of moderating effects of response strategies contingents upon response time. We interpret the results and provide implications for research and practice.

Keywords: Data breach, cybersecurity, response strategy, response time, data breach notification laws, multi-method.

INTRODUCTION

The investment of organizations in cybersecurity, which protects their business data from malicious information disclosure, is growing every year. The cybersecurity spending increased from $120 billion in 2019 to $133 billion in 2020 and is expected to reach $150 billion in 2021 (Gartner 2020; 2021). Despite this considerable investment in cybersecurity, data breaches have grown exponentially. The number of exposed records reached 30 billion in 2020, which is more than in the previous 15 years combined (Glenny 2021). The consequences of data breaches are severe for the organizations as they lose their reputation and revenue. According to a study by IBM, the average cost of a data breach in the U.S. in 2020 is $8.6 million (IBM 2020). Data breaches also impact the various stakeholders of the breached company and arouse negative reactions. Prior research has consistently noted that customers and investors are the stakeholders

who show negative behaviors after data breaches (Choi et al. 2016; Gwebu et al. 2018; Martin et al. 2017; Yayla and Hu 2011).

To alleviate the negative consequences of data breaches and recover damaged relationships with customers and investors, many companies create a response plan for these events. Security experts acknowledge the importance of a sophisticated timely response in the aftermath of a data breach to help the companies improve their impaired relationships with customers and investors (Barnes 2021; Hamilton 2019). Research also affirms the effectiveness of a company response in decreasing negative reactions to crisis events, including data breaches (Goode et al. 2017; Mansor and KaderAli 2017; Tsarenko and Tojib 2015). Although many companies recognize the importance of a response, they respond to data breaches differently. For example, in response to its data breach event in 2015, Nvidia only provided protective recommendations to customers in its data breach notification letter. Boeing, following another strategy, apologized and compensated the affected customers, in addition to the protective recommendations provided in its data breach response in 2017. Notwithstanding various responses to data breach events, the efficacy of these different responses to decrease the negative outcomes of a data breach is still unknown. Further, prior studies have indicated that customers and investors could react differently to company responses (e.g., Rasoulian et al. 2017), and, therefore, it is not clear if data breach response strategies have the same effects on these two stakeholders. Consequently, the first research objective of this study is *to investigate the repertoire of response strategies adopted by breached companies and examine their effects on customers and investors.* Evaluating the outcomes of various response strategies is important to companies so that they can employ the response strategies that have the best effect on stakeholders. Such work also contributes to crisis response management research to understand the strategies adopted in a data breach crisis.

Another facet of data breach response that companies should address after an incident pertains to the laws and regulations that government imposes on breached companies. Data breach notification laws were established in 2002, which require the breached companies to notify their affected customers about the breach. While some states demand an immediate response after the breach (e.g., California and Illinois), others allow the notifications to be sent 30 to 45 days later (e.g., Florida and Ohio)[1]. Aside from the time frame of legal notification, security experts emphasize the importance of response time and recommend announcing a data breach response in the shortest possible time (Hawthorn 2016; Matteson 2017). If the response time influences the potency of the response strategies, the breached companies should make a greater effort to expedite the delivery of the breach response. If not, they do not need to allocate more resources in the aftermath of a data breach and implement their response strategy within the legal period. Thus, the second objective of this research is *to examine the effect of response time on the impact of various response strategies*.

To fulfill the research objectives, we conduct three empirical studies. Below, we first review crisis response strategies and data breach research to understand the key findings of this area. Then, we present the findings of Study 1, which investigated breached companies' response strategies (n = 204) to identify the different patterns of response strategies that breached companies have adopted. We use expectancy violation theory (EVT) to argue that the dissatisfaction stemming from data breaches drives customers' and investors' reactions. Then, we present a moderated-moderated-mediation model (Hayes 2018) based on the EVT to examine whether various response strategies can moderate the effect of dissatisfaction on negative reactions and whether the moderating effects of such strategies depend on response time. In

[1] To review data breach notification laws, please see https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Study 2, we carried out a factorial survey (n = 811) with 15 different conditions, and, in Study 3, we conducted an event study (n = 166) to examine the effects of response strategies and times on customers and investors, respectively. We present the results of each study, followed by a discussion of implications for research and practice.

This research is expected to make several theoretical contributions. First, we contribute to cybersecurity and crisis management research by outlining different actual responses to data breaches based on the letters that companies issued after data breaches. We review these letters and create a profile of various combinations of response strategies. Second, this research extends service recovery and cybersecurity literature as there is little research that investigates customers and investors in the same study with respect to the company's response to a data security service failure. We examine customers' and investors' reactions to various response strategies, which has critical implications for managers to adopt the response strategy that effectively influences stakeholders and that decreases the costs of data breaches. Finally, this research is among the first that investigates response time based on data breach notification laws. It extends cybersecurity and crisis management research by delineating the role of time in the aftermath of a data breach crisis and discerning the contingency of response strategies on response time.

BACKGROUND AND THEORETICAL FOUNDATIONS

In this section, we review crisis response strategies and data breach research to discuss how the literature examines the major organizational responses to crises, including data breaches. We then conduct a content analysis (Study 1) to determine the actual responses that are salient in the data breach crisis context. Finally, we describe the EVT as the basis of the overall framing of our research model.

Crisis Response Strategies

A crisis is often a fundamental threat to the stability of an organization and conveys risk to significant aspects of an organization, including organizational image, legitimacy, profitability, and ultimately survival (Ulmer and Sellnow 2002). Therefore, crisis management becomes vital for any organization to maintain its stability and keep its current position in the market. Prior research argued that crisis management uses different rhetorical, impression management, and account-giving concepts to acquire an appropriate response to protect the organization's image during and after a crisis (Allen and Caillouet 1994; Benoit 1995; Caillouet and Allen 1996; Coombs 1995; 1998). As part of crisis management, organizations that face a crisis should respond to it quickly because stakeholders and the media demand immediate, thorough, and qualified responses from the organization (Hegner et al. 2016). Crisis management research emphasizes that crises almost always provoke a bad impression of the focal organization and cause stakeholders to engage in negative behaviors. For instance, Wangenheim (2005) found that a crisis can cause customers to be unhappy and spread negative word-of-mouth (WOM)—that is, negative communication with others about the organization and its products—which then keeps potential new customers away from the organization. However, when an appropriate strategy is adopted after the crisis, the negative outcomes of the incident can be considerably decreased (Borah et al. 2020; Grégoire et al. 2018).

Response strategies are the symbolic resources that help organizations to protect or repair their image after a crisis (Coombs 1998). Crisis management research enumerates several response strategies with different tactics that aid the organizations during and after the crisis. In this regard, Coombs (1998) classified various response strategies and presented a defensive-accommodative response continuum based on "accepting responsibility for the crisis" and "attempting to repair the damage." These responses can also be categorized based on their tactics

and level of remorse into defensive strategies, moderate strategies, and accommodative strategies (Gwebu et al. 2018). Table 1 shows the level of remorse and tactics of each response strategy.

Table 1. Response Strategies and Tactics

Strategy	Objective	Level of Remorse	Tactic	Definition
Defensive	This strategy focuses on the denial of the crisis or responsibility for the crisis.	Low	Attack on the Accuser	The organization confronts the person or group who claims that a crisis exists.
			Denial	The organization states that no crisis exists and explains why the organization has not encountered a crisis.
			Excuse	The organization claims that the crisis was not the organization's fault.
Moderate	This strategy minimizes the perceived severity of the crisis instead of influencing the attribution of responsibilities.	Medium	Justification	The organization claims that there was no serious damage.
			Ingratiation	The organization takes actions to make stakeholders like the organization.
Accommodative	This strategy accepts responsibility and seeks to remedy the situation.	High	Corrective Action	The organization tries to repair the damage from the crisis or take steps to prevent a repeat of the crisis.
			Apology	The organization clearly apologizes for the occurrence of the crisis.
			Compensation	The organization offers monetary or non-monetary compensations to the affected people.

Expectancy Violation Theory

We use the EVT to understand individuals' emotions and reactions following a data breach crisis. The EVT was originally developed by Burgoon and Jones (1976) to explain how individuals perceive and interpret violations of their personal space (Bevan et al. 2014). According to the EVT, humans hold expectations that characterize and frame their interactions with others, and, subsequently, they behave according to these expectations (Afifi and Metts 1998; Bevan et al. 2014; Burgoon 1993). An expectation is a consistent pattern of predictable behavior and should be considered in relation to a specific individual, context, and relationship (Burgoon 1993). Expectations can also be comprehended by understanding interactional content and relational subtext (Burgoon and Walther 1990). While content schemas are receiver-stored

knowledge about objects and events, relational schemas are the receiver's expectations for different ways people relate to one another (Housle and Acker 1979).

According to the EVT, breaking assumed rules such as information privacy violates expectations and influences relationships (Afifi and Metts 1998, p. 368). In particular, Afifi and Metts (1998) defined expectation violation as the behavior that a receiver notices as being different from the behavioral display that an individual expected. Burgoon (1978) argued that any behavior that falls outside of a range of expected behaviors produces cognitive arousal and triggers an interpretation-evaluation sequence that individuals can use to tackle negative outcomes. The expectations that are far from the expected range of behaviors are salient and provoke immediate and large changes in the relationships (Afifi and Metts 1998). Thus, violating basic expectations in any relationship provides strong negative perceptions and subsequently negative actions.

The EVT is used to investigate the impact of organizational behaviors on stakeholders. In this research domain, researchers discuss the organizational behaviors that fall outside of expected behaviors and examine how these expectancy violations affect individuals' perceptions and behaviors. For example, Cho et al. (2020) studied the public's reaction to an organization whose sustainable development violates the public's expectation and found that expectancy violation affects evaluations about the organization (i.e., credibility, attitude, and supportive behavioral intention) more than expectancy conformity. Lee and Chung (2018) applied the EVT to study corporate social responsibility (CSR) communication and found that negative emotional visuals and company-cause fit influence stakeholders' memory of CSR information. In the data breach context, Gwebu et al. (2018) used the EVT to explain an organization's failure to protect data violates its stakeholders' expectancy, which causes negative reactions such as decreasing market value.

Data breaches disclose customers' private information, and prior research argued that violating information privacy is an exemplar of confounding the individual's expectations (Afifi and Metts 1998, p. 368). Prior research also discussed that data security is one of the basic expectations of stakeholders (e.g., Ball 2001; Carroll 1991) that is violated by data breaches (Rasoulian et al. 2017). The EVT expounds on the damage caused to relationships by violating these expectations and describes consequential behaviors, which makes this theory appropriate for this study and the data breach context.

Data Breach Consequences and Responses

Consumer behavior research extensively discusses how individuals negatively react to a service failure (Borah et al. 2020; Day et al. 1981; Grégoire et al. 2018). Prior research noted that a data breach is a service failure (e.g., Goode et al. 2017; Rasoulian et al. 2017) because it aborts data security, which is a component of service quality (Lewis and Mitchell 1990; Yang and Fang 2004). In fact, a data breach represents unauthorized access to the organization's information, resulting from a compromise in information security. Data breaches possess salient characteristics that embody a major threat to company survival and that differentiate them from other types of service failure. For instance, data breaches could affect a large number of individuals representing different groups of stakeholders. They could be publicized in diverse media, and the incident cannot be easily isolated and repaired (Rasoulian et al. 2017) because the data are with cybercriminals and out of company control. Data breaches violate individuals' privacy (Malhotra and Malhotra 2011) and imperil other aspects of affected individuals' lives, especially when their identification (or other sensitive) information is stolen. Thus, due to these characteristics, stakeholders show intensively negative behaviors in the event of a data breach. For example, customers might intend to switch to another company and/or spread negative

WOM (Choi et al. 2016; Martin et al. 2017), and investors sell the breached company's stock resulting in a decline in stock price (Malhotra and Malhotra 2011; Yayla and Hu 2011).

To better understand the prior findings of data breach research, we conducted a review by identifying 71 studies from various business journals. We also reviewed service recovery studies to better understand response strategies following service failures[2]. These studies argue various strategies such as apology, appreciation, compensation, and overcompensation as effective strategies (e.g., Noone 2012; Puzakova et al. 2013; Wirtz and Mattila 2004; You et al. 2020). We found that there is limited knowledge about the best response strategy after the information protection service fails and a data breach occurs.

Studies about the effect of data breach response strategies are sparse and although these few studies shed light on the importance of response strategies, they suffer from several shortcomings. First, it is unknown if breached companies adopt a single strategy or a combination of strategies. The repertoire of strategies examined is limited, and their relative effectiveness is not clear. Second, breached companies issue notification letters to their stakeholders at different times based on the data breach notification laws in each state. However, prior studies did not consider the role of time and whether response time affects the efficacy of response strategies. Finally, response strategies could affect customers and investors differently (Marcus and Goodman 1991; Rasoulian et al. 2017) because while customers pursue event-specific satisfaction (Saad Andaleeb and Conway 2006), investors are loss-averse and seek long-term returns (Barberis and Huang 2001; Fama 1998). However, it is ambiguous whether the response strategies affect customers and investors in the same manner after data breaches, and no prior study examined these two stakeholders in the same study. Thus, to accurately represent

[2] To review the literature review procedure and findings, please refer to https://mfr.osf.io/render?url=https://osf.io/ctrfy/?direct%26mode=render%26action=download%26mode=render

strategies used in practice and examine their efficacy on customers and investors, we conducted a content analysis on official data breach response letters from breached companies.

Study 1: Content Analysis of Data Breach Response Letters

To better understand what response strategies have been adopted by organizations after facing data breaches, we investigated companies' reactions following data breaches. Our investigation found that there are two different dates to declare a data breach event: the "announcement date" and the "response date." While the announcement date is when the breach events are announced to the public, the response date is when the breached companies issue an official notification letter (that includes response strategies) to their stakeholders and legal parties. These two dates could be the same if the breached companies publicly announce their breaches and include their response strategies (e.g., compensation) in their announcements. However, there are several cases in which there is no response date, or the response date is after the announcement date (breached company issues the response letter after a third party announces the data breach). First, as it is allowed by data breach notification laws, breached companies can delay responding to data breaches, but the breach event may have already been announced by a third party (e.g., FBI, security forums, hacking groups). Second, breached companies may adopt a "no action" strategy, which refers to the organization's attempts to avoid problems by remaining silent and by not officially responding to crises (Chang et al. 2015). It is usually unveiled when the breached company intentionally decides not to announce the data breach after the incident, and the announcement is made by a third party. Finally, the data breach could be announced by a third party while the company did not discover it and was unintentionally silent. In this research, we recognize these last two cases as "no action" because the breached company was intentionally or unintentionally silent.

To identify response strategies adopted by companies after data breaches, we conducted a content analysis of data breach notification letters. We first collected information on 7250 data breaches from various sources, such as Privacy Rights Clearinghouse, Databreaches.net, PHIPrivacy.net, and the US Department of Health and Human Services. We then removed announcements that were (a) ambiguous, (b) from a non-U.S. or not-for-profit firm, and (c) from firms that were not publicly traded. Thus, we found 496 unique events from 2005–2018 that included only publicly traded U.S. organizations. The dataset incorporates different information about data breaches, such as the announcement date.

We then attempted to find the official response letters that the breached companies from our sample provided. As there is no centralized source to find the letters, we downloaded response letters incorporating response strategies from various sources, such as the websites of attorneys general[3], the breached companies' websites, security blogs, and online news websites. We finally used 204 data breach announcements with respect to official response letters from publicly traded companies that faced data breach incidents. We found that 41 companies adopted a "no action" strategy. We read each response letter from the remaining companies and analyzed the content of these letters to identify the adopted strategies (Appendix A shows an illustrative letter). We then coded[4] the adopted strategies based on the response strategies of Table 1.

Table 2 shows the response strategies in the data breach response letters, the number of letters that include any of the response strategies, and the statement example of these strategies.

[3] California Attorney General (https://oag.ca.gov/privacy/databreach/list); New Hampshire Attorney General (https://www.doj.nh.gov/consumer/security-breaches/index.htm); Washington Attorney General (https://www.atg.wa.gov/data-breach-notifications).

[4] Two independent coders identified the strategies appearing in the response letters. They first coded five letters together to reach a mutual understanding of the coding scheme. They also discussed to resolve disagreements and then coded the rest of the letters independently. We applied Perreault and Leigh's (1989) reliability index and found a high-level agreement with a score of .902. The reliability index was measured by $I_r = \{[(F/N) - (1/k)][k/(k-1)]\}^{0.5}$, for $F/N > 1/k$; where F is the frequency of agreement between coders, N is the total number of judgments, and k is the number of categories.

As Table 2 illustrates, while some breached organizations used only one strategy, the others adopted a combination of strategies. These findings provide several insights into data breach response strategies in recent years. First, the breached companies did not use defensive strategies because, when the companies issue response letters that are required by data breach notification laws, they accept that a data breach happened and do not take the defensive position (e.g., denying or attacking the accuser). We also did not find that the breached companies adopted moderate strategies, per se, and if companies use such strategies, they are in conjunction with accommodative strategies. Accommodative strategies are the main strategies of breached companies that have a higher level of remorse and responsibility (see Table 1), which can be broken down into specific strategies (i.e., corrective action, apology, compensation).

Finally, while prior research discussed how corrective actions are mainly the company's efforts to minimize the negative consequences of a crisis and attempt to prevent a similar crisis in the future (Coombs 1998), we found that in a data breach crisis, corrective actions require customers' actions as well. For example, breached companies ask customers to replace their credit cards or change their passwords, and, in the meantime, the company would implement new security measures and hire security professionals. Further, we found that even though compensation is included in the apology response type in the classification of response strategies (Coombs 1998), some breached companies offered compensation in response letters without apologizing to the affected customers. As a result, we separated apology and compensation to be two different response strategies in this study.

Table 2. Response Strategies Included in Data Breach Response Letters

Strategy Type	Number of Letters	Statement Example
Corrective Action Only	35	We retained a leading security firm to help us understand the nature and scope of the matter. Please contact your debit or credit card issuer to have your card replaced by calling the number on the back of your personal credit or debit card.
Apology Only	0	We apologize for any inconvenience this incident has caused.

Compensation Only	0	We are providing you with two years of credit monitoring at no charge. To activate your free credit monitoring, please call the number below and it will be set up for you.
Corrective Action + Apology	36	
Corrective Action + Compensation	40	
Apology + Compensation	0	
Corrective Action + Apology + Compensation	52	

RESEARCH MODEL AND HYPOTHESES

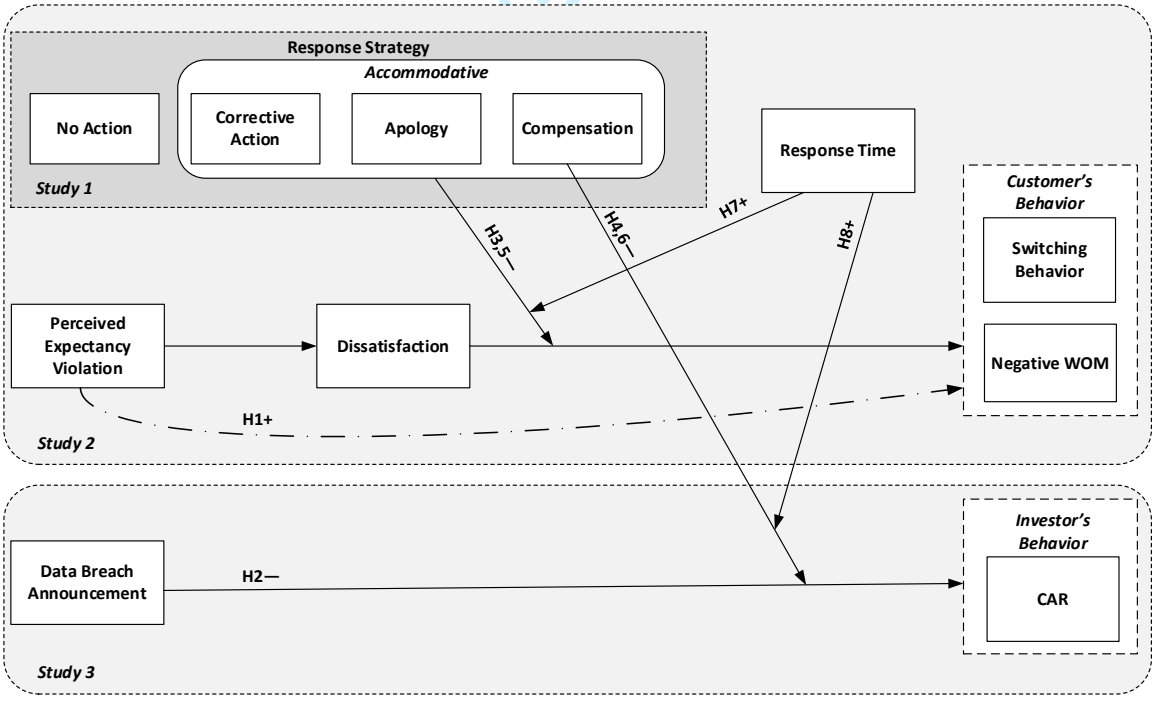
We present a moderated-moderated-mediation model of the effects of response strategies and times on customers' behaviors based on prior discussions of crisis response strategies, the content analysis of data breach response letters, and the EVT (Figure 1). In such a model, the moderation of the mediation effect by one variable is contingent upon a second moderator, which represents a three-way interaction effect (Hayes 2018). Figure 1 illustrates our model that includes moderating effects of response strategies and times on customers' and investors' behaviors separately.

Consistent with the EVT framing, we first argue that dissatisfaction stemming from data disclosure mediates the effect of information protection expectancy violation on the customers' behaviors. Prior research on consumer complaining behavior found that when customers become dissatisfied with a company, they take punitive actions (for a review, see İstanbulluoğlu et al. 2017). Switching behavior and negative WOM are common punitive behaviors resulting from a data breach (Choi et al. 2016; Martin et al. 2017), which are included in the model (Figure 1). We also discuss that investors show a poor market return performance following a data breach announcement, which leads to negative cumulative abnormal returns (CAR)[5]. CAR is the sum of the difference between the market's return and the company's return (Yayla and Hu 2011). We

[5] Although we do not hypothesize the effects of perceived expectancy violation and dissatisfaction on investor's behavior, we believe that investors recognize data breaches as an unexpected behavior that creates financial uncertainty, which leads to the selling of company stock.

then discuss how the effect of response strategies found in Study 1 can moderate the magnitude of the mediation effect (Muller et al. 2005; Preacher et al. 2007) and the effect of announcements on CAR.

In addition to the response strategies found in the content analysis of response letters, some organizations do not respond to the data breaches and try to cover up the incident. As such, we incorporate "no action" as another breached organization response strategy to compare its effect with the effects of other adopted strategies. The companies also respond to data breaches at different points in time. While some companies respond to their data breaches immediately, others delay notifying the stakeholders about the event. The response time is proposed to affect the strength of the moderating effect of response strategies and is included in the research model (Figure 1).



Note. The dashed line shows the indirect path.

Figure 1. Data Breach Response Strategy, Response Time, and Stakeholders' Behaviors

Customers' and Investors' Behaviors Following a Data Breach

According to the logic of EVT, when the communicator violates expectancies to a degree that exceeds the receiver's sensitivity, the violation is posited to intensify the receiver's arousal (Burgoon and Hale 1988). If the violations lead to sensitive and private information disclosure, they immediately arouse cognitive beliefs that change or terminate the relationship (Afifi and Metts 1998). Accordingly, when customers provide their personal information to companies as a requirement for purchasing products or receiving services, they expect that the organizations stringently protect their information. The social norm in any customer–provider relationship is that the private information of each party is not revealed by the other party. In a data breach incident, when customers find out that their information is disclosed, and criminals such as hackers have access to their information, their negative emotions regarding the breached companies will be aroused. In this regard, Beaudry and Pinsonneault (2010) categorized emotions surrounding IT events based on opportunity, threat, perceived lack of control over expected consequences, and perceived control over expected consequences. When the event is perceived as a threat and there is a lack of control over the expected consequences, emotions of "loss" are aroused (Beaudry and Pinsonneault 2010). Data breach events arouse these emotions because customers perceive these events as threats, and they are not able to control the consequences of disclosing their information, potentially to cybercriminals. Along with emotions of loss, research on customer complaining behavior constantly finds that dissatisfaction is prompted by negative feelings towards a company when a service fails (Day and Landon 1977; İstanbulluoğlu et al. 2017; Kim et al. 2010). A data breach is an exemplar of a service failure (Goode et al. 2017) as the data breach violates customers' expectations of the company to protect their information. Thus, customers become dissatisfied with their relationships with the breached companies.

Research on the customer–provider relationship shows that dissatisfaction impacts post-event behaviors. For instance, Zeelenberg and Pieters (2004) found that when customers are dissatisfied with the company in any way, they show punishing actions, such as switching to another company and spreading negative WOM. In the aftermath of a data breach, customers show negative behaviors by taking negative actions. For example, after revealing that 50 million Facebook users' private information was collected in 2014 by a political data firm that was associated with Donald Trump's 2016 presidential campaign, an online campaign with #DeleteFacebook spread negative words about Facebook and encouraged people to delete their Facebook accounts (Montgomery 2018). Consistent with EVT, we posit that when a data breach incident violates customers' expectations about company data protection, dissatisfaction as an emotion of loss is aroused and ultimately prompts the customer to switch to another company and spread negative WOM. Thus, we hypothesize that:

> **H1:** Dissatisfaction mediates the relationship between customers' perceived expectancy violation and customer's behavior (i.e., switching behavior and negative WOM).

Investors use all available information to value a company in the stock market, and when there is new information about a company, investors re-value the company accordingly (Yayla and Hu 2011). The announcements about the company have a profound effect on investors because investors are not commonly aware of the company's internal working and, thus, the announcements form investors' beliefs about the company (Teo et al. 2016). When a data breach occurs and the news of the breach is announced, it conveys a message to the public that the company was incapable of protecting organizational information against security threats. The company's inability to protect against security attacks and information loss signal unexpected company behavior to investors, creating uncertainty. As such, investors react negatively because they expect expensive lawsuits and a negative public image due to data breaches that result in financial losses (Gwebu et al. 2018). Investors also perceive the data breach events as the costs

that have a substantial effect on the company's ability to earn profit in the short term (Yayla and Hu 2011). Accordingly, investors would punish breached companies by selling their stocks, which is less than the expected price in the stock market. Prior research also constantly found the negative effect of data breach announcements on investors' behavior in the stock market (Malhotra and Malhotra 2011; Martin et al. 2017; Yayla and Hu 2011). Thus, we hypothesize that:

> **H2:** Data breach announcement affects investors to behave negatively toward the breached companies in the stock market and decreases CAR.

Moderating Role of Response Strategies

Organizations that encounter crises follow post-crisis strategies to alleviate negative stakeholders' behaviors and minimize the overall cost of the crisis. To choose an appropriate response strategy, managers first need to identify the response strategies available to them—as each response strategy requires specific resources—and then analyze the crisis situation (Coombs 1998). Each crisis needs a different response strategy based on its characteristics. For example, data breach events violate individuals' privacy, but the collapse of an organizational building (another crisis) threatens individuals' safety. As such, the response strategy for data breaches might differ from the strategy adopted after, for example, revealing a product defect. Based on our content analysis of the response strategies organizations adopted after data breaches, we found that, while some organizations did not respond to data breaches, others predominantly adopted accommodative strategies (Table 2).

Prior research investigated the effects of response strategies following crises and found that accommodative response strategies impact perceptions and behaviors after a crisis. For instance, Chang et al. (2015) found that response strategies have positive effects on customers' perceptions and behaviors and that accommodative strategies can decrease the likelihood of customers engaging in negative WOM. In the context of information privacy violation, Bansal

and Zahedi (2015) investigated the company responses that can repair trust after online privacy violation and found that apology as an accommodative strategy affects repaired trust more than a "no action" strategy.

In addition to customers, investors are influenced by crises and following company actions. In this regard, behavioral finance research investigates investors' decision-making with respect to company responses. This research enumerates several characteristics specific to investors that differentiate them from other stakeholders. According to the axioms of utility theory, investors are (a) completely rational, (b) able to deal with complex choices, (c) risk-averse, and (d) wealth-maximizing (Nagy and Obenberger 1994). Recent studies have also argued that investors' behavior could be irrational (e.g., herd behavior) when access to real-time information is limited and investors have insufficient time for deliberation (Jackson and Orr 2019; Nigam et al. 2018). The irrational behavior could be triggered by crisis events such as terrorist attacks, earthquakes (Brounen and Derwall 2010), and data breaches (Martin et al. 2017; Yayla and Hu 2011), characterized by high uncertainty and inadequate information (Jackson and Orr 2019). In the light of irrational behavior and data breach crisis, prior research argued that investors could have emotional reactions to data breaches (Malhotra and Malhotra 2011).

Although investor's decision-making could be affected by crisis events, research has found that company statements could manipulate investor's decision-making behavior. Positive or favorable information decreases uncertainty in the stock market and leads to stock price increase (Nigam et al. 2018). When the breached companies issue response letters that include favorable information about accommodative strategies, they signal the highest level of remorse to retain customers. As investors avoid uncertainty, customer retention ensures more stable future financial performance and lower associated costs (Anderson and Mansi 2009). Thus,

investors reward company responses that have positive sentiments and signal stable financial performance in the future (Connelly et al. 2011; Teo et al. 2016).

Given the above discussions of customers and investors, we argue that with the same level of stakeholders' dissatisfaction after a data breach, the companies that are responsive to the incident by expressing their remorse and accepting responsibility experience a lower level of negative outcomes than the breached companies that are apathetic. This is mainly because accepting responsibility as an accommodative strategy was found to be the optimal communication strategy (Dean 2004). As such, the breached companies can decrease the negative outcomes of data breaches by employing accommodative strategies (i.e., corrective action, apology, and compensation), and these will be superior to a "no action" strategy. Thus, we hypothesize that:

> **H3:** Accommodative response strategies (corrective action, apology, compensation, and a combination thereof) negatively moderate the relationship between dissatisfaction and customer's behavior (i.e., switching behavior, and negative WOM), such that when these responses are provided, the relationship becomes weaker.
>
> **H4:** Accommodative response strategies (corrective action, apology, compensation, and a combination thereof) negatively moderate the relationship between data breach announcement and CAR, such that when these responses are provided, the relationship becomes weaker.

Among various crisis response strategies (Table 1), compensation is the only tangible benefit that a firm can offer to its stakeholders to restore the loss (Davidow 2003). Tangible benefits can be more easily perceived, and providing compensation demonstrates a higher level of remorse and accountability. Compensation also promotes distributive justice, which is the appropriateness of the outcomes discerned by stakeholders after a data breach (Rasoulian et al. 2017). Compensation was posited to offset the customer's total cost (Grewal et al. 2008) and was found to be the best strategy in comparison with other strategies (e.g., Borah et al. 2020). In the data breach context, Goode et al. (2017) investigated the Sony PlayStation Network data breach

and found that offering compensation after data breaches can greatly influence individuals' behaviors. Based on this discussion, we believe that compensation is more effective than apology and corrective action to decrease the negative consequences of data breaches. Thus, we hypothesize that:

> **H5:** The moderating effect of compensation is stronger than (a) corrective action and (b) apology on the relationship between dissatisfaction and customer's behavior (i.e., switching behavior, and negative WOM).
>
> **H6:** The moderating effect of compensation is stronger than (a) corrective action and (b) apology on the relationship between data breach announcement and CAR.

Moderating Role of Response Time

Since 2002, data breach notification laws have been enacted irregularly and have changed over time in the U.S. In general, the law requires breached companies to notify their stakeholders about the breach and explain the type of disclosed information. While the laws in many states share some core similarities, state legislators have decided to pass laws that best protect the interests of stakeholders in their respective states. As a result, some states have more stringent laws and demand more severe penalties for violations. For example, while California requires the breached companies to immediately respond to data breaches, some other states allow the breached company to delay their responses. For instance, Florida allows the breached organizations to prompt the stakeholders within 30 days after the data breach incident, and Alabama and Ohio allow 45 days. In addition to the response delay officially considered in the data breach notification laws of many states, some organizations do not respond to their data breaches and try to hide the events from public scrutiny. For example, Uber was hacked in 2016, and the personal information of 57 million customers and drivers was stolen by cybercriminals. Uber did not respond to the data breach and instead paid the hackers $100,000 to cover up the incident (Chappell 2018). However, security experts highly recommend that the breached organizations respond to data breaches as soon as possible to boost the efficacy of their response

strategies and assuage negative reactions to the incidents (Hawthorn 2016; Matteson 2017). Research also emphasizes that the response time to the crisis should be as short as possible. Coombs (2006) argued that crisis managers should inform stakeholders immediately of what to do to protect themselves. Ulmer and Sellnow (2002) discussed that the organization should act quickly to illustrate in good faith that it is going to follow through on the pledges or promises it communicates. If the companies do not respond to the crisis immediately, another party, such as journalists, competitors, or security groups, might reveal the data breach[6] through Twitter and Facebook, increasing the negative aftereffects. In the world of public perception, the first mover has the advantage of keeping control of the narrative (Temin 2015).

We believe that when a response strategy is provided with delay after the announcement, it could give the impression that the breached company provided that response after they realized the customers' dissatisfaction. On the other hand, when the breached company responds quickly, it demonstrates good faith, honesty, and a higher level of remorse. It also shows that the company is more prepared to recover from the failure. Therefore, although the response strategies can weaken the relationship between negative emotions about the data breach and negative behaviors, their efficacy is subject to the timing of when the breached companies issue the response letters. Thus, we hypothesize that:

> **H7:** Response time impacts the moderating effect of accommodative response strategies on the relationship between dissatisfaction and customer's behavior (i.e., switching behavior, and negative WOM), such that early accommodative responses affect that relationship more than late accommodative responses.
>
> **H8:** Response time impacts the moderating effect of accommodative response strategies on the relationship between data breach announcement and CAR, such that early

[6] In 2018, *The New York Times* and *The Observer* reported that Cambridge Analytica Ltd (CA) had gained access to and used personal data about Facebook users from an external researcher who had told Facebook he was collecting it for academic purposes. The personal data of up to 87 million Facebook users were acquired—without their consent— for political advertising purposes. This data breach event is known as "Facebook–Cambridge Analytica data scandal," which precipitated a massive fall in Facebook's stock price (Deagon 2018).

accommodative responses affect that relationship more than late accommodative responses.

METHODOLOGY

In this research, we examine customers' and investors' behaviors with respect to different data breach response characteristics. Given the two different stakeholders with different dynamics involved in the model, we adopted a multi-method approach by conducting two studies. In Study 2, consistent with prior security and privacy research (e.g., Vance et al. 2015), we used the factorial survey method to examine how customers would react to response strategies and response times. In Study 3, we conducted an event study to understand investors' behavior. An event study is a well-established method for examining investors' behaviors and is appropriate for analyzing the stock market's reaction following a data breach (e.g., Martin et al. 2017; Yayla and Hu 2011).

Study 2: Factorial Survey

A factorial survey method is an advanced approach to the scenario survey. Its objective is to "uncover the social and individual structures of human judgments of social objects" (Wallander 2009, p. 505). The factorial survey method differs from typical scenario-based surveys in that the description of scenarios is experimentally manipulated and varied (Vance et al. 2015). Prior research discussed how a factorial survey integrates experimental and traditional survey methods to provide a unique research method (Vance et al. 2015). The factorial survey includes dimensions of research interest that can involve several levels, similar to treatments of the experiment method. In the factorial survey method, the dimensions and levels are converted into textual scenarios to provide real-world situations for judgment and decision making (Taylor 2006).

The factorial survey also uses a statistical random sampling method like traditional surveys, but a full combination of all dimensions and levels is possible (Vance et al. 2015). The

full factorial avoids the issue of multicollinearity as the levels are orthogonal with correlations at or near zero (Jasso 2006). Orthogonality enables us to distinguish between the different effects of response strategies and time on stakeholders' behaviors. While traditional experimental designs support a limited dimension with a few levels each before becoming impractically complex, factorial surveys do not have such limitations (Rossi and Anderson 1982). In the factorial survey, each participant receives a dimension from several combined levels and gives a response based on the level (treatment) that was manipulated in that dimension. As many companies adopt a combination of responses after a data breach (Table 2), a factorial survey is an appropriate method for this research because it tests different combinations of the responses in a systematic manner. The participants of this study randomly received different dimensions with different levels based on response strategies and times.

Scenario Design

To create our factorial survey, we provided two sets of scenarios to describe a data breach event (scenario A) and the response strategy and time (scenario B), as shown in Appendix B. We used scenarios that "present subjects with written descriptions of realistic situations and then request responses on a number of rating scales that measure the dependent variables of interest" (Trevino 1992, pp. 127–128). First, participants were asked to provide the name of a company that they *actually use* and need to provide personal information to receive a service/product. Then, the participants were shown scenario A to imagine a data breach happened in the company they mentioned earlier, and their personally identifiable information (PII) was stolen[7] due to the data breach (see Appendix B). Subsequently, the participants answered the survey items

[7] Data breach notification laws mainly require notifying stakeholders only when PII is stolen. Although data breach notification laws of each state might describe PII differently, most states agree that PII includes a resident's name, along with a Social Security number, driver's license or state identification card number, a financial account, debit, or credit card number, access code, or passwords to access financial accounts (Skeath and Kahn 2019). Thus, we included credit card information as the exemplar of PII in the scenario A.

regarding the independent variables of the research model. After this, scenario B was provided, which described the response strategy and time (see Appendix B). After reading scenario B, the participants answered the items of dependent variables of the model. Since we used the factorial survey, a full combination of all factors was possible. Thus, we considered a full combination of corrective action, apology, compensation, and response time, plus the control group (no action), which resulted in a series of 2 x 2 x 2 x 2 + 1 = 17 between-subjects factorial survey. However, as we needed to analyze the effects of response times only in conjunction with response strategies, we eliminated two conditions of response times (their direct effects) in our scenario design and, finally, used 15 groups for further analyses. We provided different scenario Bs (Appendix B) for 14 combinations of response strategies and times and examined "no action" strategies by not presenting scenario B. The participants were randomly assigned to one of these 15 groups. We also used age, gender, internet experience, data breach experience, and data breach media exposure as the control variables because their importance is acknowledged in prior information disclosure research (e.g., Malhotra et al. 2004). We adapted the scales for the constructs in the model from prior literature, as described in Appendix C.

Data Collection Procedures

Our data collection follows a systematic approach that constitutes three phases: pretest, pilot study, and primary study. In the pretest phase, we solicited feedback on the survey from five IS researchers who had Ph.D. degrees. They gave us several suggestions about the scenarios and the clarity of the survey items. We also found that the manipulations were not salient in the scenarios, and the manipulation check for response time did not pass. Therefore, we conducted a verbal protocol and reviewed the questions one by one to ensure the clarity of items. Then, we revised the scenarios and made the survey items clearer and more appropriate to the data breach context based on the suggestions and verbal protocol. After revising the factorial survey, we sent

the survey back to the five IS researchers. This time, they noted that the scenarios and survey items were much clearer, and the manipulation check was also successful. We then conducted a pilot study with 110 respondents who were similar to our respondents in the main study. We used the pilot study to do preliminary analyses, such as reliability and validity of constructs, clarity of scenarios, and manipulation checks. In this stage, the response time manipulation check required us to change the early response time from 48 to 24 hours for the primary study.

For the primary study, we initially collected 1000 responses from CloudResearch by monetarily incentivizing U.S. respondents. The requirement to participate in this study was being an adult over 18 years of age who provides personal information to purchase products/services from retail outlets. We removed the responses that did not correctly answer the security questions, manipulation questions, or took the survey in a very short time (i.e., less than five minutes). Finally, the sample size of the primary study data was 811 for further analyses, which was ample to have the power of 0.9, with a medium-size effect and 0.05 significance level, for each of 15 groups of the factorial survey (Liang et al. 2019). Demographics of the primary study participants (Appendix D) show a fairly equal spread of gender, age, marriage, internet experience, income, and education among the study participants. We also found that 85% of respondents personally experienced at least one data breach event[8].

RESEARCH MODEL TESTING RESULTS

We estimated the structural model with partial least squares (PLS) and used Smart-PLS 3.2 to conduct analyses in two stages. In the first stage, we tested whether the measures used as the operationalization of the model constructs were reliable and valid (the measurement model). After establishing the adequacy of the measurement model, we proceeded to the second stage

[8] This indicates that these participants could personally relate their data breach experiences to the scenarios.

and estimated the path coefficients of the research model (the structural model). Finally, we compared path coefficients across multiple groups using multigroup analysis (MGA). The subsequent sections report the results for these stages.

Study 2 Results

Before testing the structural model, we conducted several preliminary analyses, such as manipulation checks and common method variance (CMV), and we tested the measurement model (Appendix E). The results confirm the adequacy of the measurement model (Appendix E). We then analyzed the base relationships of the model with the "no action" group that represents the control group. As discussed earlier, a response to the data breach event is not provided in the "no action" group so that we could examine whether various response strategies are impactful. Table 3 shows the results of testing the base relationships of the model with reasonable explanatory power ($R^2_{\text{Switching Behavior}} = 0.28$ and $R^2_{\text{Negative WOM}} = 0.27$). Table 3 shows that perceived expectancy violation ($\beta = 0.42$, $p < 0.001$) positively affects dissatisfaction. Customers' dissatisfaction with the company after a data breach increases switching behavior ($\beta = 0.50$, $p < 0.001$) and negative WOM ($\beta = 0.43$, $p < 0.001$). While perceived expectancy violation does not *directly* affect switching behavior and negative WOM (Table 3), it *indirectly* increases ($\beta = 0.38$, $p < 0.001$) switching behavior and ($\beta = 0.28$, $p < 0.001$) negative WOM through dissatisfaction (Table 4). Thus, dissatisfaction fully mediates the relationship between perceived expectancy violation, switching behavior, and negative WOM, supporting H1. We also found that gender ($\beta = 0.08$, $p < 0.05$) and internet experience ($\beta = -0.19$, $p < 0.05$) affect negative WOM. Data breach experience increases ($\beta = 0.06$, $p < 0.01$) switching behavior and ($\beta = 0.05$, $p < 0.05$) negative WOM, and data breach media exposure ($\beta = 0.11$, $p < 0.01$) influences negative WOM. The results show that the effects of age on the DVs are not significant.

Table 3. Structural Model Estimates for the Base Relationships

	Dissatisfaction	Switching Behavior	Negative WOM

Age	-0.04	0.00	-0.04
Gender	0.04	0.01	0.08**
Internet Experience	0.00	0.00	-0.19*
Data Breach Experience	0.02	0.06**	0.05*
Data Breach Media Exposure	0.18***	0.05	0.11**
Perceived Expectancy Violation	0.43***	-0.03	0.00
Dissatisfaction		0.52***	0.43***
R^2	0.23	0.29	0.25

** p < 0.05; ** p < 0.01; *** p < 0.001.*

Table 4. Indirect Paths Results

	Switching Behavior	Negative WOM
Perceived Expectancy Violation→ Dissatisfaction	0.23***	0.19***

** p < 0.05; ** p < 0.01; *** p < 0.001.*

Multigroup Analysis

We conducted MGA to test the moderation effects of our study because prior research argues that MGA is the appropriate method to estimate the moderating effects when the moderator variable is a discrete variable (Eberl 2010; Henseler 2007; Sarstedt et al. 2011). In MGA, the discrete variable divides the sample data into a group of sub-samples, and in each separate sub-sample, the same PLS path model is analyzed (Eberl 2010; Henseler 2007). The moderators are discrete variables, leading us to analyze the PLS path model using MGA. We divided our sample data into groups of sub-samples based on different data breach response strategies and response times. However, the interpretations of PLS MGA results can be misleading if PLS confounds the difference in path coefficients with differences in latent construct composition (Carte and Russell 2003). As such, multigroup comparisons require measurement invariance establishment to ensure the validity of results (Millsap 2011). If there is a significant difference in the variance of constructs between two groups, the difference in path coefficients is due to differences in the contents of constructs, misrepresenting the results. Thus, we followed Henseler et al.'s (2016) invariance of composite models (MICOM) measurement approach, which requires analyzing three components: (a) configural invariance, (b) compositional invariance, and (c) the equality of composite mean values and variances. Before

analyzing MGA, we tested MICOM for all two-by-two groups based on hypotheses testing. We also tested the difference in item loadings. The results confirm the invariance of composite models[9].

We then analyzed MGA by comparing different groups of response strategies and response times. Table 5 shows the effect of dissatisfaction on the outcome variables in each group, and Table 6 shows MGA results. To test H3 and the moderating effect of accommodative strategies, we combined all groups of corrective action, apology, and compensation. Table 5 shows that the effect of dissatisfaction on both switching behavior and negative WOM in the accommodative response strategies condition is lower than in the "no action" condition. Table 6 shows that this difference in values of the dissatisfaction effect (no action vs accommodative strategies) is significant. In other words, accommodative response strategies decrease the effect of dissatisfaction on switching behavior and negative WOM. Thus, H3 is supported. "Compensation only" response significantly decreases the effect of dissatisfaction on customers' behaviors (Tables 5 and 6). "Corrective action only" response does not moderate the relationship between dissatisfaction and customers' behaviors, but "apology only," similar to compensation, negatively moderates the effect of dissatisfaction on switching behavior and negative WOM. Table 5 shows that the moderating effect of compensation is not stronger than apology. Thus, H5a is supported, but H5b is not supported. For H7, we tested whether the moderating effect of accommodative response strategies differs in early and late response times. Tables 5 and 6 show that, compared to late response strategies, the lambda values of early accommodative response strategies are significant. The moderating effect of accommodative response strategies is

[9] To see the results, please refer to https://mfr.osf.io/render?url=https://osf.io/nfsrz/?direct%26mode=render%26action=download%26mode=render

significant only when these responses are provided early (not late). Therefore, response time affects the moderating effect of accommodative response strategies, supporting H7.

Table 5. Structural Model Estimates for Different Groups

Groups	Dissatisfaction→ Switching Behavior	Dissatisfaction→ Negative WOM	Sample Size	R^2
No action	0.66***	0.57***	105	0.45
Accommodative Strategies	0.48***	0.41***	706	0.28
Apology only	0.45***	0.42***	101	0.26
Corrective Action only	0.65***	0.57***	105	0.44
Compensation only	0.42***	0.41***	98	0.26
Early Accommodative Strategies	0.44***	0.34***	352	0.24
Late Accommodative Strategies	0.53***	0.47***	354	0.35

*** $p < 0.001$.

Table 6. Multigroup Comparisons

Comparing samples	Dissatisfaction→ Switching Behavior	Dissatisfaction→ Negative WOM	Hypothesis
	Δ	Δ	
No action — Accommodative Strategies	+0.18*	+0.16*	H3
No action — Apology	+0.21*	+0.15*	H5
No action — Corrective Action	+0.01	+0.00	
No action — Compensation	+0.24*	+0.16*	
Apology — Compensation	+0.03	+0.01	
No action — Early Accommodative Strategies	+0.22*	+0.23*	H7
No action — Late Accommodative Strategies	+0.13	+0.10	

* $p < 0.05$.

Study 2 Post-Hoc Analysis

We conducted several post-hoc analyses to dig deeper into the effect of response strategies and times on switching behavior and negative WOM. First, we investigated if the response strategies have an additive effect and if their combination has a more positive effect than when they are provided separately. To do so, we examined the moderating impact of the response strategy that includes the combination of apology, corrective action, and compensation. The results[10] show that the combination of all response strategies does not have an additive

[10] To see the results, please refer to https://mfr.osf.io/render?url=https://osf.io/mqzyr/?direct%26mode=render%26action=download%26mode=render

effect, and the effect of compensation or apology is no less than when they are combined. Second, as "apology-only" and "compensation-only" strategies have negative moderating effects, we examined if these moderating effects depend on response time. We examined the moderating effect of apology and compensation with early and late response times and found that the effect of these response strategies is significant only when they are provided with an early response time.

Study 3: Event Study

Methodology

We evaluated the effects of data breach response strategies and response times on the investors' behavior in the stock market (i.e., abnormal stock returns) by conducting an event study. An event study adopts the efficient market hypothesis, which states that a stock price at a particular point in time reflects all relevant information up to that time (Fama 1998). Prior research conducted event studies to examine investors' behavior following data breaches (e.g., Martin et al. 2017; Yayla and Hu 2011). We followed the convention estimation method, as described in Appendix F.

Data Collection

To analyze the relationship between data breaches and stock returns, we used the dataset of data breaches and official response letters that we collected for Study 1. However, the event study is subject to confounding events. As the hypotheses of this study require estimating longer event windows, we controlled for an array of confounding events from around −1 to +35, including dividend declarations, contract signings, earnings information, mergers, acquisitions, and utilizing new technologies (e.g., big data, cloud computing). We used the Lexis-Nexis business news database to identify the confounding events and dropped 38 announcements

accordingly. Finally, we used 166 data breach announcements in conjunction with the corresponding response letters for further analysis.

Study 3 Results

In the event study, the stock market reaction is measured by cumulative abnormal returns (CAR). Thus, we used *Eventus*® (Cowan Research 2007) to calculate CARs in this research (see Appendix F for the estimation method). Figure 2 shows that the mean of CARs remains negative beyond 30 days of the data breach announcement day. The analyses of data breach notification letters also show that many breached companies respond to data breaches several days after the announcements of the data breaches. Therefore, we estimate CARs within longer event windows in addition to short event windows.

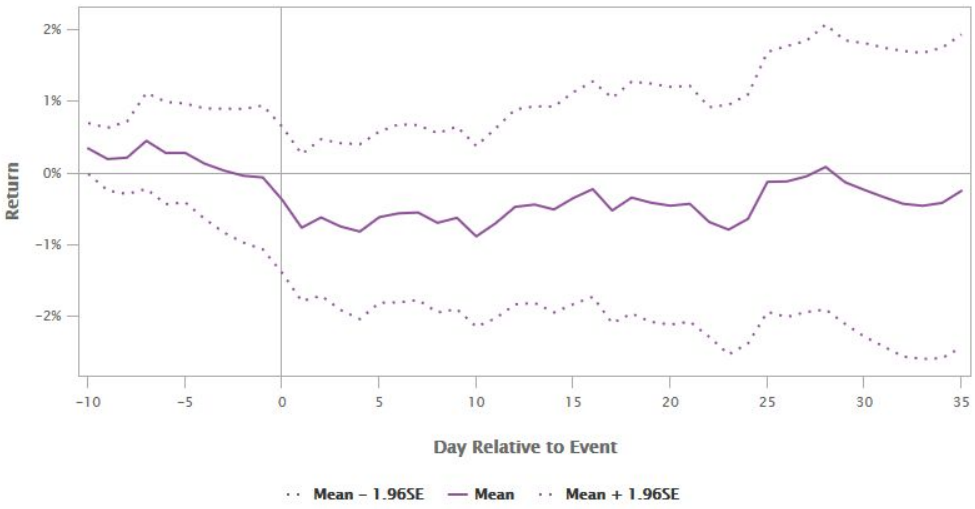


Figure 2. Cumulative Abnormal Returns (%): Mean & 95% Confidence Limits

Table 7 shows the results of the event study estimation for the full sample size with several different event windows, the mean of the CAR, and precision weighted CAAR[11]. According to Table 7, the mean of the CAR is negative for the event windows, which confirms the negative effect data breach announcements have on stock prices. Specifically, for one day

[11] Precision-weighted CAAR is an average standardized cumulative abnormal return (average SCAR).

before and after the data breach announcement (−1, 1), the mean of the CAR for all firms is −0.78%. Figure 2 shows that the mean of all CARs remains negative beyond 30 days of the data breach announcement day. We then investigated the longevity of the announcements' negative effects by analyzing longer event windows. The results show that the mean of the CAR for (−1, 32) event window is −0.73%, confirming the longevity of the negative effect of data breach announcements. Thus, as the CAR is negative from day 0 to day 32, H2 is supported.

Table 7. Results from event analyses using the full sample

Event Windows	Sample Size	Mean CAR	Precision Weighted CAAR	Patell's Z Test
(-1, 0)	166	-0.44%	-0.42%	-2.715**
(-1, 1)	166	-0.78%	-0.66%	-3.440***
(-1, 2)	166	-0.70%	-0.64%	-2.894**
(-1, 3)	166	-0.84%	-0.63%	-2.566**
(-1, 30)	166	-0.49%	-0.96%	-1.538$
(-1, 32)	166	-0.73%	-1.09%	-1.701*
(-1, 35)	166	-0.55%	-0.90%	-1.349$

*Note. $p <0.10, * p < 0.05, ** p < 0.01, *** p <0.001.*

Analysis of Effect by Response Strategies

We investigated the effect of response strategies on the relationship between data breach announcements and stock prices using the analysis of sub-samples. To test whether accommodative response strategies are effective, we divided the sample into (a) the events where the announcements include the breached company's response (accommodative strategy); and (b) the events where the announcement comes without any response (no action). As a result, to accurately capture the effect of response strategies at the time of the announcement, we only estimated shorter windows. We further divided the events with accommodative strategies into sub-samples based on the type of strategy (i.e., corrective action, compensation, and apology) to compare with the "no action" strategy. Finally, we also estimated two non-parametric tests—the rank test (Corrado 1989) and the jackknife test (Giaccotto and Sfiridis 1996)—because prior research recommended that non-parametric tests be estimated for the sample sizes below 50 in event studies (Yayla and Hu 2011), which is consistent with the size of our sub-samples.

Table 8 shows that when a data breach of a company is announced but the breached company does not provide any response on the day of the announcement (no action strategy), the mean of the CAR (−1, 1) is −0.96%. When accommodative strategies are announced on the same day of the data breach announcement (we found that both announcements usually come in the same letter), the mean of the CAR (−1, 1) is −0.60%. As both "no action" and accommodative strategies have significant negative CARs, we ran a t-test to examine if accommodative strategies significantly decrease the negative effect data breach announcements have on the CAR. The results [t (164) = 1.98, $p = 0.04$] show that accommodative strategies can significantly decrease the negative effect that data breach announcements have on the CAR. Thus, H4 is supported. While corrective action only has a significant negative CAR (-0.96%, $p < 0.05$), the results of the parametric and non-parametric tests (Table 8) show that compensation and apology do not have significant effects on CARs. Table 8 shows that while compensation is more effective than corrective action only, its efficacy is not better than that of an apology as they both have insignificant values. Thus, H6a is supported, but H6b is not supported.

Table 8. Results from event analyses of response types

Response Strategy	Event Windows	Sample Size	Mean CAR	Precision Weighted CAAR	Patell's Z Test	Rank Z Test	Jackknife Z Test
No action	(-1, 0)	37	-0.56%	-0.59%	-1.846*	-1.188	-1.405$
	(-1, 1)	37	-0.96%	-0.82%	-2.100*	-1.533$	-1.574$
	(-1, 2)	37	-0.70%	-0.88%	-1.945*	-1.456$	-1.643$
	(-1, 3)	37	-1.15%	-0.96%	-1.920*	-1.573$	-1.790*
Accommodative	(-1, 0)	129	-0.30%	-0.30%	-1.685*	-1.583$	-1.062
	(-1, 1)	129	-0.60%	-0.53%	-2.393**	-2.280*	-1.952*
	(-1, 2)	129	-0.50%	-0.45%	-1.765*	-1.690*	-1.414$
	(-1, 3)	129	-0.57%	-0.41%	-1.445$	-1.603*	-1.108*
Corrective Action Only	(-1, 0)	28	-0.70%	-0.82%	-2.003*	-2.344**	-2.329**
	(-1, 1)	28	-1.37%	-1.24%	-2.486**	-2.840**	-3.088**
	(-1, 2)	28	-2.02%	-1.81%	-3.143***	-3.569***	-3.689***
	(-1, 3)	28	-1.07%	-1.23%	-1.910*	-2.466**	-2.117*
Corrective & Compensation	(-1, 0)	29	-0.07%	-0.11%	-0.29	-0.253	-0.049
	(-1, 1)	29	-0.77%	-0.56%	-1.197	-1.012	-0.904
	(-1, 2)	29	-0.69%	-0.46%	-0.851	-0.727	-0.527

	(-1, 3)	29	-1.50%	-0.73%	-1.214	-1.17	-0.788
Corrective & Apology	(-1, 0)	25	-0.02%	0.09%	0.214	0.17	0.63
	(-1, 1)	25	0.28%	0.40%	0.802	0.756	0.823
	(-1, 2)	25	0.71%	0.59%	1.024	0.841	1.135
	(-1, 3)	25	0.59%	0.54%	0.836	0.569	0.649

*Note. $p < 0.10, * p < 0.05, ** p < 0.01, *** p < 0.001.*

Analysis of Effect by Response Time

In order to investigate the effect of response time on the efficacy of response strategies, we divided the sample into the responses that are derived from the data breach announcements (early responses) and the responses that are provided after data breach announcements (late responses). Table 9 shows the descriptive of late response time events.

Table 9. Descriptive of Late Response Events

	Sample Size	Mean	S.D.	Median	Min	Max
Late Response (Days)	37	10.5	8.71	14	3	30

The full sample results (Table 7 and Figure 2) show that the data breach announcement's negative effect on the mean of the CAR has longevity and remains negative even after 30 days. However, we tested whether early responses are more effective and have shorter negative effects. To compare the means of the CARs between early and late responses, we estimated longer event windows (−1, 30), (−1, 32), and (−1, 35) because the maximum late response day is 30 (Table 9). To this end, we divided the sample into two sub-samples (early responses and late responses) and compared them with "no action". Figure 3 shows that the event windows (−1, 30), (−1, 32), and (−1, 35) incorporate early response events as well as late responses that were delivered on different days after the data breach announcements.

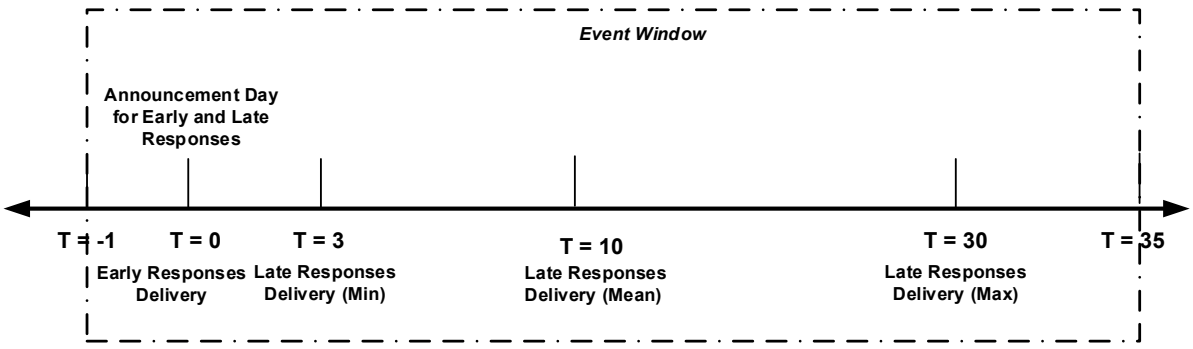


Figure 3. Early and Late Responses

Table 10 shows that while the means of the CARs for early response events are small and insignificant, those for late responses are large and significant. For example, the mean of CAR for late responses (−1, 35) is −2.64%. As the means of CARs for "no action" and late responses are negative and significant (Table 8 and 10) but the mean of CARs for early responses is insignificant (Table 10), we could conclude that early responses decrease the negative effect of announcements on CAR more than late responses. Response time affects the effectiveness of accommodative response strategies. Thus, H8 is supported.

Table 10. Results from event analyses of response time

Response Time	Event Windows	Sample Size	Equal-Weighted Market Index				
			Mean CAR	Precision Weighted CAAR	Patell's Z Test	Rank Z Test	Jackknife Z Test
Early Response	(-1, 30)	129	-0.07%	-0.78%	-1.088	-0.368	-1.058
	(-1, 32)	129	-0.19%	-0.81%	-1.094	-0.551	-1.154
	(-1, 35)	129	0.04%	-0.52%	-0.675	-0.347	-0.95
Late Response	(-1, 30)	37	-2.04%	-1.89%	-1.508$	-1.712*	-1.154
	(-1, 32)	37	-2.79%	-2.37%	-1.821*	-2.041*	-1.458$
	(-1, 35)	37	-2.84%	-2.64%	-1.946*	-2.069*	-1.488$

*Note. $p < 0.10, * p < 0.05.*

Study 3 Post-Hoc Analysis and Robustness Test

As empirical research on the longevity of the data breach effect is lacking, we conducted a long-term event study to understand how long the negative effects of data breaches last. The conventional approach to conduct a long-term event study is to estimate buy-and-hold abnormal return (BHAR), but prior research discussed that calendar-time abnormal return (CTAR) is a

superior approach (e.g., Barua and Mani 2018; Mitchell and Stafford 2000). Consequently, we used both BHAR and CTAR to conduct the long-term event study (Appendix G). We found that the negative effects of data breaches last for only six months. These results may suggest that people are no longer concerned about the data breach effects after six months[12].

To understand whether the combination of all strategies depreciates the negative effect of data breach announcements on the mean of CARs more than compensation and apology, we conducted a short-term event study with the sub-sample of "corrective & compensation & apology". We found that the effects of strategies are not additive, and the combination of corrective, compensation, and apology is not more effective than separate compensation and apology strategies, which is consistent with the results of Study 2. We also conducted several robustness tests by using Fama-French estimation methods to ensure the quality of the findings (Appendix G). The results of the robustness tests confirm the results of the event study.

DISCUSSION

The number of records exposed by data breaches is on the rise and breached companies adopt different response strategies after a data breach event. In this study, we applied the EVT to explain how stakeholders' expectations of companies' data protection are violated by data breaches and how this violation leads to adverse effects. We then sought to examine whether response strategies and times affect stakeholders' behavior. Table 11 shows the summary of hypothesis testing. These findings along with the results of post-hoc analyses provide new insights into research and practice, as discussed next.

[12] We also investigated the effect of data breaches on annual revenues. We collected data from Compustat but we were not able to find data for 12 companies in the breach years. We compared the averages of three annual revenues: the year the data breach occurred (Y), one year before (Y-1), and one year after the data breach (Y+1). The ANOVA results [F (2, 461) = 0.39, p= 0.67] show that there is not a significant difference among the three averages of annual revenues. In other words, data breaches did not significantly decrease the average of annual reviews in the breach year and the year after. These results, consistent with the findings of the long-term event study, show that the effect of data breach disappears in less than one year.

Table 11. Summary of Hypothesis Testing

Hypothesis	Result	Study
H1: Dissatisfaction mediates the relationship between customers' perceived expectancy violation and customer's behavior.	Supported	Study 2: Factorial Survey
H2: Data breach announcement decreases CAR.	Supported	Study 3: Event Study
H3, H4: Accommodative response strategies moderate the effects on the outcome variables.	Supported	Study 2: Factorial Survey Study 3: Event Study
H5a, H6a: The moderating effect of compensation is stronger than corrective action.	Supported	Study 2: Factorial Survey Study 3: Event Study
H5b, H6b: The moderating effect of compensation is stronger than apology.	Not supported	Study 2: Factorial Survey Study 3: Event Study
H7, H8: Response time impacts the moderating effect of accommodative response strategies.	Supported	Study 2: Factorial Survey Study 3: Event Study

Implications for Research

This study provides several implications for research based on the investigation of company responses and the findings of data analyses. First, this research contributes to information security research by examining if different stakeholders of a company react to a security phenomenon in the same manner. Prior data breach studies distinctively examine either customers (e.g., Choi et al. 2016; Goode et al. 2017) or investors (e.g., Yayla and Hu 2011; Gwebu et al. 2018). However, customers and investors could react differently to a company data breach response because they have different goals and decision-making behaviors (Jackson and Orr 2019; Nigam et al. 2018; Rasoulian et al. 2017). The research model of this study shows the dynamics of customers' and investors' behaviors following a data breach with respect to different response strategies and times. *Interestingly, this research found that customers and investors are similarly influenced by the same response strategies and times.* The results of the short-term event study show that within a few days after a data breach response, the stock market reacts differently to each of the various response strategies, in a manner that is similar to how customers react. For example, while prior research asserted that investors tend to react unfavorably to apologies because it is an admission of blame that could lead to lawsuits (Cohen 1999; Robbennolt 2003), we found that, like customers, investors embrace apologies and show a favorable reaction in the stock market after an apology. The alignment between customers' and

investors' reactions to data breach response strategies suggests that different stakeholders could evaluate a data breach response in the same manner. Another possible explanation is that many investors are either also customers of the breached company (Malhotra and Malhotra 2011) or have experienced data breaches and responses as customers of other companies, leading them to perceive and evaluate response strategies like customers.

Second, the EVT argues that after expectation violation, individuals act positively or negatively depending on the severity of the violation of their expectations (Burgoon and Jones 1976). Data security is a basic expectation of any stakeholder (Ball 2001; Carroll 1991), and violating this expectation is considered a service failure. We found that expectation violation due to data breaches leads to dissatisfaction in their relationship with the company. Furthermore, prior research reasoned that dissatisfaction could arise from external factors that cannot be controlled by companies (İstanbulluoğlu et al. 2017; Jacoby and Jaccard, 1981) and we found that data breaches are an external source of dissatisfaction. Prior research also contended that, when stakeholders become dissatisfied with a company, they take punitive actions against the company (Day et al. 1981). While this is reflected in our study, we found that the negative consequences of dissatisfaction due to data breaches do not last long; they remain only for six months. This corresponds well with the case study of a data breach at Target which found that the perceptions of Target's brand returned to a pre-data-breach level after six months (Dubé 2016). In this short time frame, stakeholders decide whether to take action against the breached company. This decision can be understood from two perspectives. First, the EVT discusses that when a behavior violates the expectation, it triggers cognitive arousal, and individuals follow an interpretation–evaluation sequence to decide on negative actions (Burgoon 1978). Second, complaining behavior research argues that dissatisfied individuals need to make physical and cognitive efforts to take negative actions, which impacts their decision on whether to take such

actions (Huppertz and Mower 2014). However, our findings reveal that external stimuli such as company responses can intervene in this decision-making process following reports of dissatisfaction—but only if the stakeholders evaluate the response as a signal of remorse and regret.

While prior studies elucidated the effect of company responses and how stakeholders engage with responses, most empirical studies in this area either do not use the actual responses of the breached companies (e.g., Bansal and Zahedi 2015; Goode et al. 2017), or they use broad categories of responses, such as accommodative, moderate, and defensive (Gwebu et al. 2018). The content analysis of response letters shows that accommodative strategies are the crux of data breach responses, and breached companies use either one or a combination of corrective action, apology, and compensation. While some prior research found that accommodative strategies are not influential on investors (e.g., Gwebu et al. 2018), we discovered that accommodative strategies could affect both customers and investors. However, the effectiveness depends on the type of accommodative strategy. We found that while corrective action is *not* effective, apology and compensation are impactful on *both* customers and investors.

Third, information privacy literature constantly argues that compensation and providing monetary incentives can lure individuals to disclose their sensitive information, even at the risk of losing information (e.g., Dinev et al. 2015; Smith et al. 2011). While information privacy literature asserts the effectiveness of compensation *before* information loss, this research found that compensation could also be effective *after* information loss by keeping the company's position in the stock market and reducing the likelihood of customers' switching behavior and negative WOM. However, even though prior research argued that compensation is the most effective response strategy after a service failure (Davidow 2003; Puzakova et al. 2013), we found that compensation is *not* more effective than an apology when responding to a data breach

incident. The apology and compensation strategies are different in two ways: (a) while apology expresses concern for victims, compensation offers the affected customers something to offset the suffering (Coombs and Holladay 2008), and (b) apology enhances the interactional justice perception, but compensation increases distributive justice perception (Smith et al. 1999). Despite these differences, the findings of this research show that neither of these strategies outweighs the other one. We also found that the combination of all three response strategies (corrective action, apology, and compensation) is not more impactful than compensation and apology alone. Adding more responses adds more costs but does not considerably increase the positive effects. These findings suggest that customers and investors simply want to see that the breached company is regretful, which explains why the provision of a financial offering is not more influential than an apology.

Finally, to the best of our knowledge, this is the first study that investigates the impact of response time (that occurs within the parameters of notification laws) after a data breach incident. Prior crisis management studies discussed that companies should respond to the crisis in the shortest possible time (e.g., Coombs 2006), but these studies have not examined this in the data breach context. This research found that response time *plays a vital role* after a data breach event and that the efficacy of response strategies on customer and investor behavior depends on time. The findings show that the moderating effects of accommodative responses are significant when breached companies provide them immediately. We found that accommodative strategies will lose their potency if companies employ these strategies one month after the announcement of data breaches. These results suggest that response time is seen as another signal that the breached company cares about the customers and is determined to minimize losses. Although data breach notification laws allow breached companies to delay response notifications, when companies provide response notifications late, customers infer that the breached company is

apathetic about the incident. Stakeholders might also perceive the breached company as being incapable of making a quick responsive decision about the data breach or delegate the response to external forces, such as media and regulations. The findings also indicate that response expediency is not substitutable with response strategies—providing a more comprehensive form of response at a later time is not more effective than a single response strategy provided at an earlier time.

Implications for Practice

This study has several implications that assist managers in choosing the right strategic plan. First, some companies remain silent and do not respond to data breaches, but we found that this strategy is harmful to companies; results show that breached companies should take responsibility for what happened to their customers' information and opt for accommodative strategies. However, when choosing an accommodative strategy plan, managers should be cautious about the type of strategy they adopt. We suggest that managers do not employ corrective action only and instead, at the very least, use this strategy with other forms of accommodative responses. While we found that one-fifth of companies included "corrective action only" in their response letters on the announcement date (Table 2), this strategy is not able to retain customers and prevent affected people from commenting negatively about the breached company. It also adversely affects the company's current stock price in the market.

Second, while we found that apology and compensation can be sufficient for sustaining stakeholders and preventing the spread of negative words after a data breach incident, each of these strategies requires different resources (Coombs 1998). This study suggests that apology *is as effective* as compensation and can help companies to decrease the negative consequences of a data breach event with a response strategy that requires fewer resources (i.e., apology). This finding is especially important for companies with a smaller budget. However, the effectiveness

of apology in our study relates to only two stakeholders, and managers might need to use other strategies to influence other stakeholders' behaviors. As such, this study suggests that managers include an apology in their notification letters when responding to data breaches.

Finally, the findings of this study emphasize that communication with affected stakeholders is important, but this communication should take place as soon as possible after a data breach. The results of this study show that accommodative strategies impact customers and investors only when breached companies respond immediately to the incident. Although data breach notification laws in some states allow breached companies to notify affected customers until 45 days after the incident, this study suggests that breached companies respond much earlier. Otherwise, accommodative responses would not be potent enough to assuage customers and investors from taking negative actions. The findings regarding response times can also be helpful for legislators to revise data breach notification laws and consider customers' and investors' expectations for companies to respond earlier to data breaches. Any response notification after 45 days will not be effective, even if it is within the parameters of the state laws.

Limitations and Future Research

There are some limitations in this study that provide opportunities for future research. First, we only examined the set of accommodative strategies and contrasted them with "no action" strategies because they were the only ones that breached companies adopted. However, future research can examine specific defensive (e.g., attacking the accuser) and moderate (e.g., justification) strategies to examine if these are more effective than accommodative strategies. Future research can also investigate why a company adopts a particular strategy (e.g., apology) and the challenges that a company faces when adopting a strategy. Another facet of adopting response strategies is stakeholder notification of breach and response strategies, but we do not

know the most effective communication channel for informing stakeholders. Future research can examine different media (e.g., social media, company's website, TV, newspapers) to identify influential media. As delayed responses have adverse negative effects, future research can investigate how to shorten the discovery time of data breaches and decrease the response time. Future research can also examine if contextual factors (e.g., firm size, industry type, market share) affect the strength of response strategies. Further, our breached data in the scenario was credit card information and we provided both free credit card monitoring and purchase discounts in the factorial survey to examine compensation. Future research can examine different kinds of sensitive information and separate types of compensation to understand their relative effectiveness. Moreover, although we checked CMV with two methods, our factorial survey might still suffer from CMV because the participants rated the items of the scenarios at the same point in time. Therefore, future data breach research using factorial surveys can avoid CMV by, for example, temporally separating the measurement of the predictors and outcome variables. We also examined customers' intentions after a data breach, but intentions might not lead to behaviors. Additionally, future research can examine customers' behaviors after a data breach incident.

CONCLUSION

Despite considerable investment in information security, companies face data breaches and subsequently lose many customers and investors. Breached companies adopt various response strategies to mitigate the negative consequences of data breaches. In this research, we did a content analysis of actual response letters to identify the response strategies that the breached companies adopted. We then studied the extent to which these strategies mitigated adverse consequences of the data breach on two stakeholders: customers and investors. Using a factorial survey with 15 conditions (n=811) and an event study (n=166), we examined the

adverse effects of the breach on customers and investors respectively and then analyzed how response strategies and times affect these relationships. The results indicate that data breaches violate stakeholders' expectations, which increases dissatisfaction and ultimately leads to the intention of spreading negative words about or leaving the company, as well as a negative reaction in the stock market. However, companies can positively manipulate customers' intentions and investors' behavior through accommodative response strategies. While strategies that took corrective actions were not effective, strategies that showed regret (apology) were just as effective as strategies that provided monetary benefits (compensation). These results were remarkably consistent across the two types of stakeholders. Importantly, the immediacy of response, regardless of the data breach laws, increases the impact of these strategies.

REFERENCES

Afifi, W. A., and Metts, S. 1998. "Characteristics and Consequences of Expectation Violations in Close Relationships," *Journal of Social and Personal Relationships* (15:3), pp. 365-392.

Allen, M. W., and Caillouet, R. H. 1994. "Legitimation Endeavors: Impression Management Strategies Used by an Organization in Crisis," *Communications Monographs* (61:1), pp. 44-62.

Angst, C. M., Block, E. S., D'arcy, J., and Kelley, K. 2017. "When Do IT Security Investments Matter? Accounting for The Influence of Institutional Factors in The Context of Healthcare Data Breaches," *MIS Quarterly* (41:3), pp. 893-916.

Arcuri, M. C., Gai, L., Ielasi, F., and Ventisette, E. (2020). "Cyber Attacks on Hospitality Sector: Stock Market Reaction," *Journal of Hospitality and Tourism Technology* (11:2), pp. 227-290.

Ball, K. S. 2001. "The Use of Human Resource Information Systems: A Survey," *Personnel Review* (30:6), pp. 677–693.

Banker, R. D., and Feng, C. 2019. "The Impact of Information Security Breach Incidents on CIO Turnover," *Journal of Information Systems* (33:3), pp. 309-329.

Bansal, G., and Zahedi, F. M. 2015. Trust Violation and Repair: The Information Privacy Perspective. *Decision Support Systems* (71), pp. 62-77.

Barberis, N., & Huang, M. 2001. "Mental Accounting, Loss Aversion, and Individual Stock Returns," *Journal of Finance* (56:4), pp. 1247–1292.

Barnes, R. 2021. "Data Breach Notification Laws: How to Manufacture a Confident Response," Retrieved from https://www.nist.gov/blogs/manufacturing-innovation-blog/data-breach-notification-laws-how-manufacture-confident-response.

Barua, A., and Mani, D. 2018. "Reexamining the Market Value of Information Technology Events," *Information Systems Research* (29:1), pp. 225-240.

Beaudry, A., and Pinsonneault, A. 2010. "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use," *MIS Quarterly* (34:4), pp. 689-710.

Benoit, W. L. 1995. *Accounts, Excuses, and Apologies: A Theory of Image Restoration Strategies*. Albany: State University of New York Press.

Bentley, J. M. 2018. "What Counts as An Apology? Exploring Stakeholder Perceptions in A Hypothetical Organizational Crisis," *Management Communication Quarterly* (32:2), pp. 202-232.

Bevan, J. L., Ang, P. C., and Fearns, J. B. 2014. "Being Unfriended on Facebook: An Application of Expectancy Violation Theory," *Computers in Human Behavior* (33), pp. 171-178.

Borah, S. B., Prakhya, S., and Sharma, A. 2020. "Leveraging Service Recovery Strategies to Reduce Customer Churn in An Emerging Market," *Journal of the Academy of Marketing Science* (48:5), pp. 848-868.

Burgoon, J. K. 1978. "A Communication Model of Personal Space Violations: Explication and an Initial Test," *Human Communication Research* (4:2), pp. 129-142.

Burgoon, J. K. 1993. "Interpersonal Expectations, Expectancy Violations, And Emotional Communication," *Journal of Language and Social Psychology* (12:1-2), pp. 30-48.

Burgoon, J. K., and Hale, J. L. 1988. "Nonverbal Expectancy Violations: Model Elaboration and Application to Immediacy Behaviors," *Communications Monographs* (55:1), pp. 58-79.

Burgoon, J. K., and Jones, S. B. 1976. "Toward a Theory of Personal Space Expectations and Their Violations," *Human Communication Research* (2:2), pp. 131-146.

Burgoon, J. K., and Walther, J. B. 1990. "Nonverbal Expectancies and the Evaluative Consequences of Violations," *Human Communication Research* (17:2), pp. 232-265.

Caillouet, R. H., and Allen, M. W. 1996. "Impression Management Strategies Employees Use When Discussing Their Organization's Public Image," *Journal of Public Relations Research* (8:4), pp. 211-227.

Carroll, A. B. 1991. "The Pyramid of Corporate Social Responsibility: Toward the Moral Management of Organizational Stakeholders," *Business Horizons* (34:4), pp. 39–48.

Carte, T., and Russell, C. J. 2003. "In Pursuit of Moderation: Nine Common Errors and Their Solutions," *MIS Quarterly* (27:3), pp. 479-501.

Chang, H. H., Tsai, Y. C., Wong, K. H., Wang, J. W., and Cho, F. J. 2015. "The Effects of Response Strategies and Severity of Failure on Consumer Attribution with Regard to Negative Word-Of-Mouth," *Decision Support Systems* (71), pp. 48-61.

Chappell, B. 2018. "Uber Pays $148 Million Over Yearlong Cover-Up of Data Breach," Retrieved from https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach.

Cho, M., Park, S. Y., and Kim, S. 2020. "When an Organization Violates Public Expectations: A Comparative Analysis of Sustainability Communication for Corporate and Nonprofit Organizations," *Public Relations Review*, in press, DOI: https://doi.org/10.1016/j.pubrev.2020.101928.

Choi, B. C., Kim, S. S., and Jiang, Z. 2016. "Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems*, (33:3), pp. 904-933.

Cohen, J. R. 1999. "Advising clients to apologize," *Southern California Law Review* (72), pp. 1009–1070

Coombs, W. T. 1995. "Choosing the Right Words: The Development of Guidelines for the Selection of the "Appropriate" Crisis-Response Strategies," *Management Communication Quarterly* (8:4), pp. 447-476.

Coombs, W. T. 1998. "An Analytic Framework for Crisis Situations: Better Responses from A Better Understanding of the Situation," *Journal of Public Relations Research* (10:3), pp. 177-191.

Coombs, W. T. 2006. "The Protective Powers of Crisis Response Strategies: Managing Reputational Assets during a Crisis," *Journal of Promotion Management* (12:3-4), pp. 241-260.

Coombs, W. T., and Holladay, S. J. 2008. "Comparing Apology to Equivalent Crisis Response Strategies: Clarifying Apology's Role and Value in Crisis Communication," *Public Relations Review* (34:3), pp. 252-257.

Corrado, C. J. 1989. "A Nonparametric Test for Abnormal Security-Price Performance in Event Studies," *Journal of Financial Economics* (23:2), pp. 385-395.

Cowan Research, LC. 2007. "Eventus® (Version 9): Software for Event Studies and CRSP Data Retrieval/ User's Guide," Cowan Research, Ames, IA (http://www.eventstudy.com).

Davidow, M. 2003. "Organizational Responses to Customer Complaints: What Works and What Doesn't," *Journal of service research* (5:3), pp. 225-250.

Davis, M. 2019. "4 Damaging After-Effects of a Data Breach," Retrieved from https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach.

Day, R. L., Grabicke, K., Schaetzle, T., and Staubach, F. 1981. "The Hidden Agenda of Consumer Complaining," *Journal of Retailing* (57:3), pp. 86-106.

Day, R. and Landon, L. 1977. "Towards a Theory of Consumer Complaining Behavior", in Arch Woodside, J.S. and Bennet, P. (Eds), *Consumer and Industrial Buying Behavior*, North-Holland Publishing, Amsterdam.

Deagon, B. 2018. "Facebook Stock Troubles Didn't Start with Data Scandal." Retrieved from https://www.investors.com/news/technology/facebook-stock-sell-signals-cambridge-analytica-data-scandal.

Dean, D. H. 2004. "Consumer Reaction to Negative Publicity: Effects of Corporate Reputation, Response, and Responsibility for A Crisis Event," *The Journal of Business Communication*, (41:2), pp. 192-211.

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. Research Commentary—Informing Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research* (26:4), pp. 639-655.

Dubé, L. 2016. "Autopsy of a Data Breach: The Target Case (Teaching Notes)," *International Journal of Case Studies in Management* (14:1), pp. 1-21.

Eberl, M. 2010. "An Application of PLS in Multi-Group Analysis: The Need for Differentiated Corporate-Level Marketing in the Mobile Communications Industry," in *Handbook of Partial Least Squares,* V. Esposito Vinzi, W. W. Chin, J. Henseler, and H. Wang (eds.), Berlin: Springer, pp. 487-514.

Fama, E. F. 1998. "Market Efficiency, Long-Term Returns, And Behavioral Finance1," *Journal of Financial Economics* (49:3), pp. 283–306.

Gartner. 2020. "Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020," Retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem.

Gartner. 2021. "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021," Retrieved from https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem.

Giaccotto, C., and Sfiridis, J. M. 1996. "Hypothesis Testing in Event Studies: The Case of Variance Changes," *Journal of Economics and Business* (48:4), pp. 349-370.

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.

Glenny, M. 2021. "Pandemic Accelerates Growth in Cybercrime," Retrieved from https://www.ft.com/content/49b81b4e-367a-4be1-b7d6-166230abc398

Grégoire, Y., Ghadami, F., Laporte, S., Sénécal, S., and Larocque, D. 2018. "How Can Firms Stop Customer Revenge? The Effects of Direct and Indirect Revenge on Post-Complaint Responses," *Journal of the Academy of Marketing Science* (46:6), pp. 1052-1071.

Grewal, D., Roggeveen, A., and Tsiros, M. 2008. "The Effect of Compensation on Repurchase Intentions in Service Recovery," *Journal of Retailing* (84), pp. 424–434.

Gwebu, K., and Barrows, C. W. 2020. "Data Breaches in Hospitality: Is the Industry Different?" *Journal of Hospitality and Tourism Technology* (11:3), pp. 511-527.

Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," *Journal of Management Information Systems* (35:2), pp. 683-714.

Hamilton, E. 2019. "The Importance of a Timely Data Breach Response," Retrieved from https://www.techtimes.com/articles/240760/20190402/importance-timely-data-breach-response.htm.

Hawthorn, N. 2016. "The First 48 Hours: How to Respond to a Data Breach". Retrieved from https://www.infosecurity-magazine.com/opinions/the-first-48-hours-respond-data.

Hayes, A. F. 2018. "Partial, Conditional, and Moderated Moderated Mediation: Quantification, Inference, and Interpretation," *Communication Monographs*, (85:1), pp. 4-40.

Hegner, S. M., Beldad, A. D., and Kraesgenberg, A. L. 2016. "The Impact of Crisis Response Strategy, Crisis Type, and Corporate Social Responsibility on Post-Crisis Consumer Trust and Purchase Intention," *Corporate Reputation Review* (19:4), pp. 357-370.

Henseler, J. 2007. "A New and Simple Approach to Multi-Group Analysis in Partial Least Squares Path Modeling," in *PLS'7: The 5th International Symposium on PLS and Related Methods*, Ås, Norway, September 5-7, pp. 104-107.

Henseler, J., Ringle, C. M., and Sarstedt, M. 2016. "Testing Measurement Invariance of Composites Using Partial Least Squares," *International Marketing Review* (33:3), pp. 405-431.

Housel, T. J., and Acker, S. R. 1979. "Schema theory: Can it connect communication's discourse?" Paper presented at the annual meeting of the International Communication Association, Philadelphia.

Huppertz, J., and Mower, E. 2014. "Organizational Responses to Consumer Complaints: A Re-Examination of the Impact of Organizational Messages in Response to Service and

Product-Based Failures," *Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior* (27*)*, pp. 6-18.
IBM. 2020. "Cost of a Data Breach Report 2020," Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report.
İstanbulluoğlu, D., Leek, S., and Szmigin, I. T. 2017. "Beyond Exit and Voice: Developing an Integrated Taxonomy of Consumer Complaining Behavior," *European Journal of Marketing* (51:5/6), pp. 1109-1128.
Jacoby, J. and Jaccard, J. 1981. "The Sources, Meaning, And Validity of Consumer Complaint Behavior: A Psychological Analysis", *Journal of Retailing* (57:3), pp. 4-24.
Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research* (34:3), pp. 334-423.
Kim, S. H., and Kwon, J. 2019. "How Do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information?" *Information Systems Research* (30:4), pp. 1184-1202.
Kim, M. G., Wang, C., and Mattila, A. S. 2010. "The Relationship Between Consumer Complaining Behavior and Service Recovery: An Integrative Review," *International Journal of Contemporary Hospitality Management* (22:7), pp. 975-991.
Kwan, C. 2020. "Equifax Direct Payments to Members to End Class Action Could Top $500 Million". Retrieved from https://www.zdnet.com/article/equifax-direct-payments-to-members-to-end-class-action-could-top-500-million.
Lee, S. Y., and Chung, S. 2018. "Effects of Emotional Visuals and Company–Cause Fit on Memory of CSR Information," *Public Relations Review* (44:3), pp. 353-362.
Lewis, B. R., and Mitchell, V. W. 1990. "Defining and Measuring the Quality of Customer Service," *Marketing intelligence & planning* (8:6), pp. 11-17.
Liang, H., Xue, Y., Pinsonneault, A., and Wu, Y. 2019. "What Users Do Besides Problem-Focused Coping When Facing It Security Threats: An Emotion-Focused Coping Perspective," *MIS Quarterly* (43:2), pp. 373-394.
Liginlal, D., Sim, I., and Khansa, L. 2009. "How Significant Is Human Error as A Cause of Privacy Breaches? An Empirical Study and A Framework for Error Management," *Computers & Security* (28:3-4), pp. 215-228.
Manworren, N., Letwat, J., and Daily, O. 2016. "Why You Should Care About the Target Data Breach," *Business Horizons* (59:3), pp. 257-266.
Matteson, S. 2017. "8 steps to take within 48 hours of a data breach". Retrieved from https://www.techrepublic.com/article/8-steps-to-take-within-48-hours-of-a-data-breach.
Malhotra, A., and Malhotra, C. 2011. "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach," *Journal of Service Research* (14:1), pp. 44-59.
Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and A Causal Model," *Information Systems Research* (15:4), pp. 336-355.
Mansor, F., and KaderAli, N. N. 2017. "Crisis Management, Crisis Communication, and Consumer Purchase Intention Post-crisis," *Global Business & Management Research* (9:4), pp. 60-79.
Marcus, A. A., and Goodman, R. S. 1991. "Victims and Investors: The Dilemmas of Presenting Corporate Policy During A Crisis," *Academy of Management Journal* (34:2), pp. 281-305.

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.

McLeod, A., and Dolezel, D. 2018. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches," *Decision Support Systems* (108), pp. 57-68.

Millsap, R.E. 2011. *Statistical Approaches to Measurement Invariance.* Routledge, New York, NY.

Mitchell, M. L., and Stafford, E. 2000. "Managerial Decisions and Long-Term Stock Price Performance," *The Journal of Business* (73:3), pp. 287-329.

Montgomery, S. J. 2018. "People Decide to #DeleteFacebook Following Data Breach". Retrieved from https://www.complex.com/life/2018/03/people-delete-facebook-following-data-breach.

Muller, D., Judd, C. M., and Yzerbyt, V. Y. 2005. "When Moderation Is Mediated and Mediation Is Moderated," *Journal of personality and Social Psychology* (89:6), pp. 852-863.

Noone, B.M. 2012. "Overcompensating For Severe Service Failure: Perceived Fairness and Effect on Negative Word-Of-Mouth Intent", *Journal of Services Marketing* (26:5), pp. 342-351.

Perreault Jr, W. D., and Leigh, L. E. 1989. "Reliability of Nominal Data Based on Qualitative Judgments," *Journal of Marketing Research* (26:2), pp. 135-148.

Preacher, K. J., Rucker, D. D., and Hayes, A. F. 2007. "Addressing Moderated Mediation Hypotheses: Theory, Methods, And Prescriptions," *Multivariate Behavioral Research* (42:1), pp. 185-227.

Puzakova, M., Kwak, H., and Rocereto, J. F. 2013. "When Humanizing Brands Goes Wrong: The Detrimental Effect of Brand Anthropomorphization Amid Product Wrongdoings," *Journal of Marketing* (77:3), pp. 81-100.

Rasoulian, S., Grégoire, Y., Legoux, R., and Sénécal, S. 2017. "Service Crisis Recovery and Firm Performance: Insights from Information Breach Announcements," *Journal of the Academy of Marketing Science* (45:6), pp. 789-806.

Ratnam, G. 2019. "White House Cybersecurity Budget Up 5 Percent in 2020, White House Says," Retrieved from https://www.rollcall.com/news/whitehouse/cybersecurity-up-5-percent-in-2020-budget-white-house-says.

Robbennolt, J. K. 2003. "Apologies and Legal Settlement: An Empirical Examination," *Michigan Law Review* (102:3), pp. 460–516.

Rossi, P. H., and Anderson, A. B. 1982. "The Factorial Survey Approach: An Introduction," in *Measuring Social Judgments: The Factorial Survey Approach,* P. H. Rossi, and S. Nock (eds.), Beverly Hills, CA: Sage Publications, pp. 15-67.

Saad Andaleeb, S., and Conway, C. 2006. "Customer Satisfaction in the Restaurant Industry: An Examination of the Transaction-Specific Model," *Journal of Services Marketing* (20:1), pp. 3–11.

Sarstedt, M., Henseler, J., and Ringle, C. M. 2011. "Multi-Group Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results," *Advances in International Marketing* (2), pp. 195-218.

Skeath, C., and Kahn, B. 2019. "Round-Up of Recent Changes to U.S. State Data Breach Notification Laws". Retrieved from https://www.insideprivacy.com/data-security/data-breaches/round-up-of-recent-changes-to-u-s-state-data-breach-notification-laws.

Smith, A. K., Bolton, R. N., and Wagner, J. 1999. "A Model of Customer Satisfaction with Service Encounters Involving Failure and Recovery," *Journal of Marketing Research* (36:3), pp. 356-372.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.

Syed, R. 2019. "Enterprise Reputation Threats on Social Media: A Case of Data Breach Framing" *The Journal of Strategic Information Systems* (28:3), pp. 257-274.

Taylor, B. J. 2006. "Factorial Surveys: Using Vignettes to Study Professional Judgement," *British Journal of Social Work* (36:7), pp. 1187-1207.

Temin, D. 2015. "You Have 15 Minutes to Respond to A Crisis: A Checklist of Dos and Don'ts," Retrieved from https://www.forbes.com/sites/daviatemin/2015/08/06/you-have-15-minutes-to-respond-to-a-crisis-a-checklist-of-dos-and-donts/#5eb14e4e50a8.

Trevino, L. K. 1992. "Experimental Approaches to Studying Ethical–Unethical Behavior in Organizations," *Business Ethics Quarterly* (2:2), pp. 121-136.

Tsarenko, Y., and Tojib, D. 2015. "Consumers' Forgiveness After Brand Transgression: The Effect of The Firm's Corporate Social Responsibility and Response," *Journal of Marketing Management* (31:17-18), pp. 1851-1877.

Ulmer, R. R., and Sellnow, T. L. 2002. "Crisis Management and the Discourse of Renewal: Understanding the Potential for Positive Outcomes of Crisis," *Public Relations Review* (28:4), pp. 361-365.

Vance, A., Lowry, P. B., and Eggett, D. L. 2015. "Increasing Accountability through the User Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly* (39:2), pp. 345-366.

Wallander, L. 2009. "25 Years of Factorial Surveys in Sociology: A Review," *Social Science Research* (38:3), pp. 505-520.

Wangenheim, F. V. 2005. "Postswitching Negative Word of Mouth," *Journal of Service Research* (8:1), pp. 67-78.

Wirtz, J., and Mattila, A. S. 2004. "Consumer Responses to Compensation, Speed of Recovery and Apology After a Service Failure," *International Journal of service industry management* (15:2), pp. 150-166.

Yang, Z., and Fang, X. 2004. "Online Service Quality Dimensions and Their Relationships with Satisfaction," *International Journal of Service Industry Management* (15:3), pp. 302-326.

Yayla, A. A., and Hu, Q. 2011. "The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors," *Journal of Information Technology* (26:1), pp. 60-77.

You, Y., Yang, X., Wang, L., and Deng, X. 2020. "When and Why Saying "Thank You" Is Better Than Saying "Sorry" In Redressing Service Failures: The Role of Self-Esteem," *Journal of Marketing* (84:2), pp. 133-150.

Zeelenberg, M., and Pieters, R. 2004. "Beyond Valence in Customer Dissatisfaction: A Review and New Findings on Behavioral Responses to Regret and Disappointment in Failed Services," *Journal of Business Research* (57:4), pp. 445-455.

APPENDIX A— Coding of An Illustrative Response Letter Including Apology, Corrective Action, and Compensation

After investigating internal security, Boeing found a data breach that affected 36000 individuals. Boeing notified the Washington state Attorney General and officials in California, North Carolina, Massachusetts, and affected people by providing a response letter.

Global Privacy Office
The Boeing Company
P.O. Box 3707, MC: 18-19
Seattle, WA 98124-2207

02/08/2017

Example Individual
100 N. Riverside
Chicago, IL 60606

RE: Notice of Data Breach

Dear Example Individual:

This message concerns a recent data security incident that involved your information. While we do not believe your information has been or will be used inappropriately, we sincerely apologize for this incident and wanted to share the following details.

What Happened:

Boeing recently discovered that a company employee sent an email containing personal information of other employees to his non-Boeing spouse on Nov. 21, 2016. During Boeing's investigation, the employee stated that he sent a spreadsheet with the personal information to his spouse for help with a formatting issue. He did not realize the spreadsheet included sensitive personal information because that information was contained in hidden columns. We have taken steps to ensure that any copies of the spreadsheet have been destroyed, including a forensic examination of both the Boeing employee's computer and the spouse's computer to confirm that any copies of the spreadsheet have been deleted. Both the employee and his spouse have confirmed to us that they have not distributed or used any of the information.

What Information Was Involved:
The spreadsheet contained each employee's first and last name, place of birth, BEMSID, and accounting department code in visible columns, and social security number and date of birth in hidden columns.

What We Are Doing:
In addition to the efforts described above, we will require additional training on the proper handling of personal information and will be examining additional controls to further protect your personal information.

Although we do not believe your information has been or will be used inappropriately, we are offering a **complimentary** two-year membership of Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

What You Can Do:

1. **Activate your ProtectMyID account as soon as possible.**
   1. ENSURE **That You Enroll By: 05/31/17** (Your code will not work after this date.)
   2. VISIT the **ProtectMyID Web Site to enroll:** www.protectmyid.com/protect
   3. PROVIDE **Your Activation Code:** ASDF1234

   Note: A credit card is not required for enrollment.

If you have questions or need an alternative to enrolling online, please call 866-751-1324 and provide engagement number: **PC106405**.

2. Be on the alert for suspicious activity related to your accounts, credit report and financial products. You will have access to your Experian consumer credit report as part of the Experian ProtectMyID product. We recommend that you also take the following steps to protect your identity:

   - Check your other consumer reports annually. You may obtain a free copy of your credit report once every 12 months from each of the nationwide consumer reporting agencies by visiting http://www.annualcreditreport.com or by contacting the consumer reporting agencies at:
     - Experian, 866-200-6020, P.O. Box 2002, Allen, TX 75013; www.experian.com
     - Equifax, 800-685-1111, P.O. Box 740241, Atlanta, GA 30374-0241; www.equifax.com
     - TransUnion, 800-680-7289, P.O. Box 6790, Fullerton, CA 92834-6790, www.transunion.com
   - You should monitor your bank, health care, and health insurance records to ensure there are no transactions or other activity that you did not initiate or authorize. Report any suspicious activity in your records to the appropriate service provider and to one of the national credit reporting companies listed below, and ask for a fraud alert or a security freeze on your credit report. Remember to renew the fraud alerts every 90 days.
     - Experian, Fraud Hotline: 888-397-3742, P.O. Box 2002, Allen, TX 75013; www.experian.com
     - Equifax, Fraud Hotline: 877-478-7625, P.O. Box 740241, Atlanta, GA 30374-0241; www.fraudalerts.equifax.com
     - TransUnion, Fraud Hotline: 800-680-7289, P.O. Box 6790, Fullerton, CA 92834-6790; www.transunion.com; report fraud: fvad@transunion.com
   - Report any suspicious activities on your credit reports or bank, health care or health insurance records to your local police or sheriff's office and file a police report. Keep a copy of this police report in case you need it to clear your personal records.
   - You can obtain additional Information about preventing Identity Theft from the Federal Trade Commission (FTC): 877-382-4357, https://www.consumer.ftc.gov/topics/identity-theft

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5 each to place, temporarily lift, or permanently remove a security freeze.

For North Carolina Residents: You can obtain information from the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Attorney General's Consumer Hotline toll-free within North Carolina at 877-5-NO-SCAM or 919-716-6000.

On behalf of Boeing, I sincerely apologize for this incident and regret any inconvenience it may cause you. I encourage you to take advantage of the free identify theft protection service. If you have questions or concerns regarding this matter or the protections available to you, please do not hesitate to contact the Boeing Global Privacy Office at globalprivacy@boeing.com or 206-544-2406.

Sincerely,

Marie Olson

Marie Olson
Deputy Chief Privacy Officer

CODING

By reading Boeing's letter (above), we found that the letter includes all three accommodative strategies: apology, corrective action, and compensation. The following table shows how we coded the letter based on the included statements.

Response Strategy	Statement in the Letter
Apology	We sincerely apologize for this incident…
Corrective Action	We recommend that you take the following steps to protect your identity…

Compensation	We are offering a complimentary two-year membership of Experian's ProtectMYID Elite.

APPENDIX B— Scenario Design

Scenario A— Data Breach Incident

Users provide their information to companies for purchasing and using services. However, hackers can hack these companies and steal users' information, which is called a data breach. So, in this survey, we need to know your perceptions and beliefs about data breaches.

Please provide the name of one online company that you are a customer of, and you need to provide the credit card information to purchase products or get services from.

{Name of Company}

Now imagine you have just realized that the company you mentioned above (hereafter we call it "this company") has faced a major data breach. You have found out that your credit card information was disclosed due to the data breach. Please answer the rest of the questions based on this event.

Scenario B— Early Response Time and Combination of Apology & Corrective Action & Compensation

After only 24 hours *[early response time]* of the data breach event, the breached company provides the following response:

"We apologize for what happened and we strive to maintain extensive security and privacy programs *[apology]*. We are taking a number of steps (recommendations) for your protection:

We recently locked online access to your account(s). If you haven't already done so, you'll be prompted to reset your password the next time you sign in. Please make sure your new password is unique. We'll continue monitoring your account(s) for suspicious activity *[corrective action]*. We're providing two years of free credit monitoring and identity protection with TransUnion's

credit monitoring service. We also give you a 10% discount for your next purchase *[compensation]*."

APPENDIX C—Measurement

A. Measurement Items

We adapted the items of perceived expectancy violation from Affifi and Metts (1998) and those of dissatisfaction from Bhattacherje (2001). We borrowed the scales of switching behavior and negative WOM from Choi et al. (2016) and Martin et al. (2017), respectively. We believe that average customers are not aware of the details of data breach notification laws. Therefore, they do not know what state requires immediate, 30-day, or 45-day response. Moreover, these laws are for companies, not customers, and many customers might not even know the location (state) of the company that they purchase from. Thus, we believe that it is just a perception of whether a response is late, even legally. We measured response time by providing early response time (24 hours) and late response time (30 days) in textual factors. We initially chose 48 hours for early response time because practice and research recommend an immediate response to the crisis (Coombs 2006; Hawthorn 2016; Matteson 2017) but the results of pilot study analyses showed that response time manipulation check did not pass successfully because the respondents did not perceive 48 hours as an early response time. Thus, we changed the response time to 24 hours for primary study and the manipulation check passed successfully. We also chose 30 days for a long response time because it is the minimum response time among the states that allow 30 to 45 days to respond. We provided different descriptions for each of the accommodative response strategies (corrective action, apology, and compensation) in the scenarios and combined the descriptions to make 14 factors of our factorial survey. All items are 7-point Likert scales. Table C1 shows the measurement items and Table C2 shows the manipulation check questions.

Table C1. Construct Items

Constructs	Measurement	Reference

Perceived Expectancy Violation	Based on the above scenario, to what extent do you agree with the following statements. 1. I did not expect that this company could not protect my information against the data breach attack. 2. I was shocked that this company could not protect my information against the data breach attack. 3. I was surprised that this company could not protect my information against the data breach attack.	Affifi and Metts 1998
Dissatisfaction	After the data breach, how do you feel about your overall relationship with the breached company? 1. dissatisfied/ satisfied 2. displeased/ pleased 3. frustrated/ contented 4. Absolutely terrible/ absolutely delighted	Bhattacherje 2001
Switching Behavior	To what extent do you agree with the following statements after the data breach incident: 1. I will look for an alternate company. 2. I will think about switching to an alternate company. 3. I will consider an alternative company as my major service provider.	Choi et al. 2016
Negative WOM	After the data breach event, I would likely: 1. Spread negative word of mouth about the company. 2. Bad-mouth the company to my friends, relatives, or acquaintances. 3. Tell others not to choose them if asked about their products/services.	Martin et al. 2017
Data Breach Media Exposure	How much have you heard or read during the last year about data breaches and their consequences? (1 = not at all; 7 = very much)	Malhotra et al. 2004
Data Breach Experience	How many times have you personally been the victim of data breaches? (number)	Malhotra et al. 2004

Note. Responses range from 1 = "strongly disagree" to 7 = "strongly agree," unless otherwise indicated.

Table C2. Manipulation Check Questions

To what extent do you agree with these statements:
1. The response time was late.
2. The breached company apologized to you.
3. The breached company provided recommendations for protecting against the data breach consequences.
4. The breached company compensated you and offered you financial incentives.

Note. Responses range from 1 = "strongly disagree" to 7 = "strongly agree".

Appendix C References

Afifi, W. A., and Metts, S. 1998. "Characteristics and Consequences of Expectation Violations in Close Relationships," *Journal of Social and Personal Relationships* (15:3), pp. 365-392.

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

Coombs, W. T. 2006. "The Protective Powers of Crisis Response Strategies: Managing Reputational Assets during a Crisis," *Journal of promotion management* (12:3-4), pp. 241-260.

Hawthorn, N. 2016. "The First 48 Hours: How to Respond to a Data Breach". Retrieved from https://www.infosecurity-magazine.com/opinions/the-first-48-hours-respond-data.

Matteson, S. 2017. "8 steps to take within 48 hours of a data breach". Retrieved from https://www.techrepublic.com/article/8-steps-to-take-within-48-hours-of-a-data-breach.

Choi, B. C., Kim, S. S., and Jiang, Z. 2016. "Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems*, (33:3), pp. 904-933.

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.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and A Causal Model," *Information Systems Research* (15:4), pp. 336-355.

APPENDIX D— Demographics of Primary Study Participants

Demographic Variable	Category	Frequency (Percentage)
Gender	Female	403 (49.69)
	Male	408 (50.31)
Age	18-24	120 (14.80)
	25-29	176 (21.70)
	30-34	149 (18.37)
	35-44	158(19.48)
	45- 54	107(13.19)
	55-65	73(9.00)
	Over 65	28(3.45)
Marriage	Divorced	69 (8.42)
	Married	369 (45.05)
	Single	374 (45.67)
	Widowed	7 (0.85)
Internet Experience	Below 10	110 (13.43)
	10-15	162 (19.78)
	16-20	301 (36.75)
	Over 20	246 (30.04)
Income	Below $20,000	83 (10.13)
	$20,000—$39,999	211 (25.76)
	$40,000—$69,999	252 (30.77)
	$70,000—$99,999	156 (19.05)
	$100,000 and over	117 (14.28)
Education	High school or some college	325 (39.68)
	Bachelor	381 (46.52)
	Master	95 (11.60)
	Doctorate	18 (2.20)

APPENDIX E— Preliminary Analysis and Measurement Model

A potential issue in survey-based research is a common method variance (CMV) that can provide flawed results and misleading interpretations (Podsakoff et al. 2003). To check CMV,

we used Lindell and Whitney's (2001) marker variable test and Harmon's one-factor test (Podsakoff and Organ 1986). The results show that the risk of CMB is low, but that CMB remains a possibility given that these tests cannot rule out this threat. We then proceeded with checking the manipulations of the scenarios. To check the manipulation of response time, we asked the respondents if the response time was late. The results $t(810) = 10.81$, $p < 0.001$ show that the respondents differently perceived early response time ($M = 2.94$, $SD = 1.66$) and late response time ($M = 6.37$, $SD = 1.17$). To ensure the participants understood the different response strategies that appeared in the scenarios, each group received three questions related to the response strategies. The results of MANOVA show significant differences among the three response strategies (apology condition: $F[2, 307] = 92.22$, $p < 0.001$, partial $\eta^2 = 0.37$; corrective action condition: $F[2, 307] = 66.20$, $p < 0.001$, partial $\eta^2 = 0.30$; compensation condition: $F[2, 307] = 84.82$, $p < 0.001$, partial $\eta^2 = 0.35$). Thus, manipulation of response strategies was successful.

We evaluated the reliability and validity of the data based on prior recommendations (e.g., Straub et al. 2004). All the values of Cronbach alpha (α) and composite reliability (CR) exceed the recommended threshold of 0.70 (Nunnally 1978), supporting the reliability of all constructs. We found that convergent validity is supported by all values of average variance extracted (AVE) being above the threshold of 0.50. Table E1 shows discriminant validity is supported by all inter-variable correlations being below the square roots of the associated variables' AVE values (Segars, 1997). Loadings and cross-loadings also show the items differentially represent the variables of the research model[13].

Table E1. Correlation and Square-Root of Average Variance Extracted

	1	2	3	4	5	6	7	8	9
1. Age	**N/A**								

[13] For more information about preliminary analysis and measurement model, please refer to https://mfr.osf.io/render?url=https://osf.io/2fyv8/?direct%26mode=render%26action=download%26mode=render

2. Gender	-0.09	**N/A**							
3. Internet Experience	0.39***	-0.01	**N/A**						
4. Data Breach Experience	0.00	0.02	0.03	**N/A**					
5. Data Breach Media Exposure	0.08*	0.05	0.06	0.15***	**N/A**				
6. Perceived Expectancy Violation	0.05	-0.15***	0.02	-0.03	0.11**	**0.87**			
7. Dissatisfaction	-0.02	0.00	-0.01	0.03	0.24***	0.40***	**0.90**		
8. Switching Behavior	-0.04	0.02	-0.02	0.10**	0.19***	0.15***	0.49***	**0.93**	
9. Negative WOM	-0.09**	0.09**	-0.13***	0.09**	0.22***	0.15***	0.47***	0.53***	**0.93**

*Note. Diagonal is square root of average variance extracted (AVE). * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.*

Appendix E References

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86:1), pp. 114-121.

Nunnally, J. C. 1978. *Psychometric Theory*. New York, NY: McGraw-Hill.

Podsakoff, P. M., and Organ, D. W. 1986. "Self-reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp. 531-544.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and 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), pp. 879-903.

Segars, A. H. 1997. "Assessing the Unidimensionality Of Measurement: A Paradigm and Illustration within the Context of Information Systems Research," *Omega* (25:1), pp. 107-121.

APPENDIX F— Event Study Estimation Method

The common approach in event studies is to first compute stock returns on or around the date of the event under consideration. Following the convention of event studies (e.g., Yayla and Hu 2011; Martin et al. 2017), we used the equal-weighted market index return as the market return in our model and set the estimation period to 120 days, starting at t = -130 days and ending at t = -10 days, where t = 0 day represents the event date. However, it is important to make a clarification on the security event date. From the investors' perspective, the meaningful event date for a firm-specific security breach is the day when the breach becomes public knowledge, which is not necessarily the date when the breach actually occurred (Yayla and Hu 2011). As such, we carefully choose the appropriate event date for each security breach incident based on the type of breach and the context of the announcement. We estimated daily stock return for each firm using the CRSP stock price dataset over the window of [-130, -10]. We

calculated the abnormal returns for shorter windows (-1, 0), (-1, 1), (-1, 2), and (-1, 3). The logic behind these event windows is that the stock market may have "pre-announcement" information about the data breach and may react before the market closes a day before the public data breach announcement (Hovav et al. 2017). As we test the hypothesis about response time, we also calculated the abnormal returns for longer windows (-1, 30), (-1, 32), and (-1, 35).

Appendix F References

Hovav, A., Han, J., and Kim, J. 2017. "Market Reaction to Security Breach Announcements: Evidence from South Korea," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* (48:1), pp. 11-52.

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.

Yayla, A. A., and Hu, Q. 2011. "The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors," *Journal of Information Technology* (26:1), pp. 60-77.

APPENDIX G. Event Study Post-hoc Analysis and Robustness Test

A. Post-hoc Analysis

The common approach to analyzing long-term abnormal returns is using buy-and-hold abnormal returns (BHAR). However, some studies argue that BHARs may amplify underperformance by combining single period returns or they do not sufficiently account for potential cross-sectional dependence in returns, providing misleading results (e.g., Barua and Mani 2018; Mitchell and Stafford 2000). These studies suggest calendar-time abnormal returns (CTAR) as an alternative method. Thus, we estimate long-term abnormal returns with both BHAR and CTAR methods using the market model. As we previously examined the short-term effect of data breaches in the one-month period, we set the starting estimation period of long-term abnormal returns to three months and increased it to subsequent three months until one year. We also removed the confounding events for each longer period as the way we did for the short-term event study, resulting in different sample sizes. Table G1 shows the results of the

long-term event study and indicates that the results of BHAR and CTAR are consistent. The results show that after *six* months the negative effects of data breaches diminish.

Table G1. Long-Term Abnormal Returns

Period	Sample Size	BHAR		CTAR	
		Mean Value	Precision Weighted Value	Mean Value	Precision Weighted Value
3 months	163	-1.67%*	-1.83%*	-1.67%*	-2.04%*
6 months	155	-0.24%*	-2.00%*	-0.24%*	-2.39%*
9 months	148	-0.79%	-1.77%	-0.79%	-2.02%
12 months	139	-0.43%	-1.08%	-0.43%	-1.52%

*Note. * P<0.05*

B. Robustness Tests

We conducted several robustness tests to ensure the quality of the findings. While we followed prior security event studies (e.g., Martin et al. 2017) to estimate the main analyses with the market model, we conducted the Fama-French three-factor model and Fama-French-momentum four-factor model as alternative specifications. We found that the estimations of all alternative models are consistent with each other and with the market model as the main analysis of this research[14].

Appendix G References

Barua, A., and Mani, D. 2018. "Reexamining the Market Value of Information Technology Events," *Information Systems Research* (29:1), pp. 225-240.

Mitchell, M. L., and Stafford, E. 2000. "Managerial Decisions and Long-Term Stock Price Performance," *The Journal of Business* (73:3), pp. 287-329.

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.

[14] To see the results, please refer to https://mfr.osf.io/render?url=https://osf.io/mqygb/?direct%26mode=render%26action=download%26mode=render