The Role of Disclosure Specificity in Mitigating Trust Violation After a Data Breach: A Multiple Stakeholder Approach

Zhuoli Axelton
University of Wisconsin - Green Bay, axeltonz@uwgb.edu

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

Follow this and additional works at: https://aisel.aisnet.org/mwais2022

Recommended Citation
https://aisel.aisnet.org/mwais2022/2

This material is brought to you by the Midwest (MWAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MWAIS 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
The Role of Disclosure Specificity in Mitigating Trust Violation After a Data Breach: A Multiple Stakeholder Approach

Zhuoli Axelton*
University of Wisconsin – Green Bay
axeltonz@uwgb.edu

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

* authors are listed in alphabetical order; both authors contributed equally to the paper

ABSTRACT

Regulators and standard setters have urged companies to enhance the informativeness of cybersecurity risk disclosures in financial statements. Managers also have the incentive to restore public trust in their ability through quality cybersecurity risk disclosures following a data breach. However, little is known about how cybersecurity risk disclosures may influence various stakeholders' attitudes and behavior. This study examines how the perceived presence of specificity of cybersecurity risk disclosures influences the behavioral intentions of different stakeholders (i.e., investors, users, and employees) through beliefs and attitudes. Additionally, the study examines and contrasts the role of two different types of ability-based trust (i.e., trust in protecting data, and trust in conducting transactions) that impact stakeholder intentions differently. The evidence from our experiment suggests that the perceived presence of specific disclosure elements influences behavior and intentions (for all three stakeholders, users, investors, and employees) through beliefs and attitudes.

Keywords
Cybersecurity; Data breach; Belief reinforcement model; Disclosure; Specificity; Stakeholders.

INTRODUCTION AND BACKGROUND

Data breaches pose severe risks to users’ privacy and impact customers’ trust, as well as investors’ and employees’ confidence. A company that suffers a data breach has to deal with the loss of trust and confidence from not only users (Burt, 2019) but also investors (Ali, Lai, Hassan and Shad, 2021; Cheng and Walton, 2019; Kelton and Pennington, 2020; SEC, 2018), and employees (Adams, 2020; Sanders, 2019). Data breaches are known to undermine trust in the ability of a company (Bansal and Warkentin, 2021) or even government (Farrell, 2017) to protect users’ data.

Risk communication is part of a business strategy to restore credible, trusting relationships with the stakeholders, including investors (Coombs, 2014; Spence, 2020). Given the increased frequency of data breach and their relative magnitude in recent years, regulators (such as SEC) have urged companies to enhance cybersecurity risk disclosures in their financial statements (SEC, 2018). However, the informativeness of cybersecurity risk disclosures varies significantly across companies (Bansal, Zahedi and Gefen, 2015). Further, little is known about how cybersecurity risk disclosures may influence various stakeholders' attitudes and behavior following a data breach. Hence, building on the belief reinforcement model (BRM) (Song and Zahedi, 2005), we examine how the perceived presence of disclosure specificity impacts the behavioral intentions of different stakeholders – users, investors, and employees.

The BRM posits that perceived presence impacts beliefs which in turn impact attitudes and intentions. This research focuses on ability-based trust beliefs since a data breach could be considered an ability-based violation when viewed as management’s inability to effectively manage the internal processes (Bansal and Warkentin, 2021). Generally, ability-based trust has been measured in the context of conducting transactions (Bhattacharjee, 2002; Gefen and Straub, 2004). However, we argue ability-based trust in protecting data may play a more important role in influencing stakeholder intentions than ability-based trust in conducting transactions following a data breach.

Prior research suggests that disclosures with high specificity and verifiability will convey management credibility and restore higher trust than general or no disclosure (Cannon, 2021; Rosenthal, 1971). Consistent with this notion, Hope, Hu and Lu
(2016) document that higher specificity of risk disclosures benefits financial statement users more. However, no research examines how the perceived specificity of disclosures can mitigate the drop in ability-based trust and thus influence stakeholder intentions (Spence, 2020). The BRM suggests that the saliency of beliefs is specific to the individuals’ behavior under investigation (Song and Zahedi, 2005). Drawing on the BRM, we hypothesize that perceived specificity elements of cybersecurity risk disclosures directly impact the beliefs about disclosure specificity. In turn, the beliefs about disclosure specificity mitigate the drop in ability-based trust and thus influences stakeholder behavioral intentions following the data breach.

The research questions were examined using an experimental survey. Participants were first shown a fictitious e-commerce website and asked to answer questions in reference to the website. We first measured the overall trust along with ability-based trust in the website. Participants then viewed one of the three scenarios designed with varying specificity of risk disclosures about the data breach. Perceived seriousness of the breach news and the perceived presence of the specific details (date, size of the breach, type of the information stolen, and the business location) were measured next. We then measured the violated ability-based trust. Drop in the ability-based trust was computed by taking a difference of the initial and the violated ability-based trust ratings. We then measured the behavioral intentions for three different stakeholder groups – users, investors, and employees. Trust propensity and demographics were measured at the end. We intercepted several attention checks throughout the survey to ensure the participants were attentive to the scenario and the items asked.

The findings show that the perceived presence of specific disclosure reinforces belief about disclosure specificity. The belief about disclosures specificity is negatively associated with the drop in ability-based trust in protecting data. In contrast, the negative association between the belief about disclosures specificity and the drop in ability-based trust in conducting transactions is insignificant. Consistent with our hypothesis, the drop in ability-based trust in protecting data is negatively associated with stakeholder intentions for all three groups - users, investors, and employees.

The study contributes to both research and practice in the field of cybersecurity and trust rebuilding following a data breach. Our findings were pertaining to stakeholders and the perceived presence of specificity disclosures elements in the context of mitigating trust violation following a data breach.

**RESEARCH MODEL AND HYPOTHESES**

*Perceived presence of specific risk disclosure elements.* BRM suggests that "the mere presence of elements in a Web-design category is not adequate for influencing a Web customer; its presence must be perceived to create any possible impact on the Web customer's belief (Song and Zahedi, 2005, p. 1225)." Further, the saliency of beliefs is specific to the individuals' behavior under investigation. In the context of cybersecurity risk disclosures following a data breach, we argue that the perceived presence (and not actual presence) of specific disclosure elements directly impacts the underlying individual's beliefs about the specificity of the disclosure.

H1: The perceived presence of specific disclosure elements (date, size of the breach, type of information stolen, and business location) is positively associated with belief about the specificity of disclosure.

*Specificity of risk disclosure.* Disclosures with higher specificity present a complete and clear representation of reality and help deliver persuasive/communication (Rosenthal, 1971). Further, the belief that risk disclosures are specific and complete would build trust that the disclosing party will behave dependable, ethical, and in a socially appropriate manner (Gefen, Karahanna and Straub, 2003). Such beliefs would enable the trust that will help mitigate the perceived violation following a data breach, a trust-impairing event.

Data breaches have been shown to erode all three trust beliefs – ability, benevolence, and integrity (Bansal and Zahedi, 2015). However, a data breach could be considered an ability-based trust violation primarily if it were viewed as management's inability to manage the data protection processes effectively (Bansal and Warkentin, 2021). Thus, in this research, we focus on trust violations about ability-based trust. Ability-based trust is contextual because the ability is task and situation-specific (Mayer, Davis, and Schoorman, 1995). Ability-based trust in an online business is conventionally measured as the degree of one’s belief that the company is competent in conducting the transactions (Bhattacherjee, 2002). In the context of cybersecurity risk disclosures following a data breach, we argue that a company's ability to protect data is a separate construct from the ability to conduct transactions. Thus, we hypothesize that beliefs about the specificity of risk disclosures will mitigate the negative impact of ability-based trust violation following a data breach, including the ability to a) conducting transactions and b) protecting data.

H2: Following a data breach, belief about disclosure specificity will mitigate the drop in ability-based trust in (a) conducting transactions and (b) protecting data.
Trust and user intentions. Trust is an expectation that others one chooses to trust will not behave opportunistically by taking advantage of the situation. Such behaviors include privacy violations and unauthorized use of data from users (Gefen et al., 2003; Mayer, Davis and Schoorman, 1995). Trust is particularly important in online transactions because of the risk of information asymmetry between users and the business. In addition, the risks may arise from the absence of proven guarantees that the company will not engage in harmful opportunistic behaviors. Thus, building trust is a critical aspect of e-commerce.

From a user standpoint, higher trust is associated with a higher likelihood of engaging with the company. In the information age, stakeholders are increasingly interconnected. A company’s actions toward users are visible to other stakeholders, such as employees and stakeholders, and thus impact the trustworthiness of other stakeholders. In turn, a company’s trustworthiness will determine to what degree other stakeholders will assume vulnerability and engage in future exchange relationships (Crane, 2020). Therefore, a company that suffers a data breach has to deal with the loss of trust and confidence of business stakeholders, including users (Curtis, Carre and Jones, 2018), investors (Ali et al., 2021), as well as employees (Adams, 2020; Sanders, 2019).

Hence, in the context of cybersecurity risk disclosures following a data breach, we argue that a drop in the ability-based trust will negatively impact all stakeholder intentions, which includes users, investors, and employees. Further, we separately examine the effect of the drop in ability-based trust in conducting transactions vs. protecting data.

H3: Drop in trust in the ability to conduct transactions is negatively associated with (a) user intentions, (b) investor intentions, and (c) employee intentions.

H4: Drop in trust in the ability to protect data is negatively associated with (a) user intentions, (b) investor intentions, and (c) employee intentions.

Trust in the ability to protect data vs. trust in conducting transactions. Following a data breach, stakeholders (and not only users) will be more concerned about the company’s ability in protecting data than its ability in conducting transactions. Hence,

H5: Drop in ability-based trust in protecting data plays a stronger mediating role, between beliefs about disclosure specificity and behavioral intentions, than drop in ability-based trust in conducting transactions.

EXPERIMENT

A survey instrument was developed in Qualtrics. We developed the scale for perceived presence and beliefs related to specific disclosure items based on Rosenthal (1971) and Song and Zahedi (2005). Intention items were adapted from Alniacik, Alniacik and Genc (2011) and Rana, Dwivedi, Lal, Williams and Clement (2017). Perceived seriousness of news, trust propensity and ability-based trust beliefs and overall trust items were adapted from Bansal and Zahedi (2015). We identified four specific disclosure elements: date, time, location, and entity based on suggestions made by Rosenthal (1971). The study was conducted online, and data was gathered from subjects solicited through Amazon Mechanical Turk (MTurk). Data collected through
MTurk has been shown to possess high reliability and validity (Hibbeln, Jenkins, Schneider, Valacich and Weinmann, 2017). After removing incomplete and respondents who failed attention checks, we had three hundred and nine usable responses. There were 193 males and 115 females in the final sample. One person chose the other as gender. The average age of the respondents is shown in Table 1 below. We examined the data for reliability, discriminant and convergent validity, and common-method variance and found no issues. The data were analyzed using Smart PLS.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Average age</th>
<th>Std dev</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>37.326</td>
<td>10.703</td>
<td>193</td>
</tr>
<tr>
<td>Female</td>
<td>39.417</td>
<td>12.335</td>
<td>115</td>
</tr>
<tr>
<td>Other</td>
<td>26.000</td>
<td>-</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 1. Demographics

RESULTS
The findings show that the following hypotheses - H1, H2b, H4, and H5 were supported, whereas H2a and H3 were not supported. The results are shown in Figure 2 and Table 2. The control variables/paths analysis results are shown in Table 3.

![Figure 2. Results for H1–H4](image)

The results suggest that the perceived presence of specific disclosure elements impact intentions (for all three stakeholders, users, investors, and employees) through beliefs, attitude (drop in ability-based trust in protecting data), and not through drop in ability-based trust in conducting transactions. H5 was examined using indirect path analysis, thus confirming the significant mediating role of drop in ability-based trust in protecting data (see Table 2).

<table>
<thead>
<tr>
<th>Indirect Path</th>
<th>Path Coef.</th>
<th>T Stat</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mediation tests: perceived presence of elements &gt; belief about perceived specificity of disclosure -&gt; drop in ability-based trust in protecting data -&gt; investor intentions</td>
<td>0.071</td>
<td>2.174</td>
<td>*</td>
</tr>
<tr>
<td>Mediation tests: perceived presence of elements &gt; belief about perceived specificity of disclosure -&gt; drop in ability-based trust in protecting data -&gt; user intentions</td>
<td>0.070</td>
<td>2.167</td>
<td>*</td>
</tr>
<tr>
<td>Mediation tests: perceived presence of elements &gt; belief about perceived specificity of disclosure -&gt; drop in ability-based trust in protecting data -&gt; employee intentions</td>
<td>0.059</td>
<td>2.152</td>
<td>*</td>
</tr>
</tbody>
</table>
Mediation tests: perceived presence of elements > belief about perceived specificity of disclosure -> drop in ability-based trust in conducting transactions -> investor intentions

<table>
<thead>
<tr>
<th>Path</th>
<th>Path Coeff</th>
<th>T-stat</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust1 -&gt; Drop in Ability-based trust in protecting data</td>
<td>0.148</td>
<td>1.831</td>
<td>ns</td>
</tr>
<tr>
<td>Trust1 -&gt; Drop in Ability-based trust in conducting transactions</td>
<td>0.178</td>
<td>2.047</td>
<td>*</td>
</tr>
<tr>
<td>Trust propensity -&gt; Drop in Ability-based trust in protecting data</td>
<td>-0.250</td>
<td>2.795</td>
<td>**</td>
</tr>
<tr>
<td>Trust propensity -&gt; Drop in Ability-based trust in conducting transactions</td>
<td>-0.218</td>
<td>2.249</td>
<td>*</td>
</tr>
<tr>
<td>Verifiability -&gt; Drop in Ability-based trust in protecting data</td>
<td>-0.202</td>
<td>1.980</td>
<td>*</td>
</tr>
<tr>
<td>Verifiability -&gt; Drop in Ability-based trust in conducting transactions</td>
<td>-0.338</td>
<td>3.708</td>
<td>***</td>
</tr>
<tr>
<td>Verifiability -&gt; Employee intentions</td>
<td>0.480</td>
<td>7.009</td>
<td>***</td>
</tr>
<tr>
<td>Verifiability -&gt; Users intentions</td>
<td>0.415</td>
<td>7.468</td>
<td>***</td>
</tr>
<tr>
<td>Verifiability -&gt; Investors intentions</td>
<td>0.447</td>
<td>8.188</td>
<td>***</td>
</tr>
<tr>
<td>Seriousness -&gt; Drop in Ability-based trust in protecting data</td>
<td>0.363</td>
<td>3.368</td>
<td>***</td>
</tr>
<tr>
<td>Seriousness -&gt; Drop in Ability-based trust in conducting transactions</td>
<td>0.267</td>
<td>2.898</td>
<td>**</td>
</tr>
</tbody>
</table>

Note: significance was examined for two-tail p values; *** p<.001; ** p<.01; * p<.05; ns: not significant

Table 2. Results for H5

DISCUSSION AND CONCLUSION

The results confirm the hypotheses and provide several theoretical and practical implications. A significant contribution of this research has been to demonstrate that in the context of a data breach, the trust violation negatively impacts the behavioral intentions for all three stakeholders – users, investors, and employees. The findings are in line with the argument that in the information age, stakeholders are increasingly interconnected, where a company’s actions toward one stakeholder can impact members of the stakeholder ecosystem (Crane, 2020). The findings also contribute to the trust and disclosure literature by establishing how disclosure specificity beliefs mitigate trust violation following a data breach. Moreover, the results provide evidence that the perceived presence of specificity of risk disclosure elements, namely, date, size of the breach, type of information stolen, and business location, is important in developing beliefs regarding the perceived specificity of the disclosures. Results also show that in the context of data breaches, trust in the ability in protecting data plays a more vital role than trust in the company’s ability in conducting transactions. Future research should be conducted to check this finding in other contexts. The study supports the SEC’s call to promote quality cybersecurity risk disclosures to restore credibility and trust by increasing transparency following a data breach. In addition, the study provides practical guidance for managers regarding the importance of being transparent in risk disclosures in their communications (annual reports and media) with various stakeholders.

REFERENCES


